日本国特許庁
JAPAN PATENT OFFICE

19. 2. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月２１日

出願番号
Application Number: 特願２００３－０４５１０７
[ST. 10/C]: [ＪＰ２００３－０４５１０７]

出願人
Applicant(s): 松下電器産業株式会社

２００４年　３月２５日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０２４５３６

【書類名】　特許願
【整理番号】　2022540519
【提出日】　平成15年 2月21日
【あて先】　特許庁長官　　殿
【国際特許分類】　G06F　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　原田　俊治
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理システム、記録媒体及び情報処理装置

【特許請求の範囲】

【請求項１】　ソフトウェアを記録している記録媒体と、前記ソフトウェアを内部に記録し、前記ソフトウェアに従って動作する情報処理装置とから構成される情報処理システムであって、

前記記録媒体は、

ソフトウェアを記憶している通常記憶手段と、

前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、

耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備え、

前記情報処理装置は、

前記ソフトウェアを記憶するための領域を備える記憶手段と、

前記記録媒体から前記許可指示を取得する取得手段と、

取得した前記許可指示に応じて、前記記録媒体から前記ソフトウェアを取得して前記記憶手段に書き込み、又は前記記憶手段に記憶されている前記ソフトウェアを非活性化する制御手段とを備える

ことを特徴とする情報処理システム。

【請求項２】　ソフトウェアを記録している記録媒体であって、

ソフトウェアを記憶している通常記憶手段と、

前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、

耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアン

インストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段と

を備えることを特徴とする記録媒体。

【請求項３】　前記通常記憶手段は、ソフトキーを用いて暗号化された暗号化ソフトウエアを記憶しており、

前記セキュア記憶手段は、前記ソフトキーを含む前記ライセンス情報を記憶しており、

前記耐タンパモジュール手段は、インストール可と判断する場合に、前記セキュア記憶領域に記憶されているライセンス情報からソフトキーを抽出し、抽出したソフトキーをセキュアに出力する

ことを特徴とする請求項２に記載の記録媒体。

【請求項４】　前記セキュア記憶手段は、前記ソフトウェアの署名データを含む前記使用条件に係る前記ライセンス情報を記憶しており、

前記耐タンパモジュール手段は、インストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報から前記署名データを抽出し、抽出した前記署名データを出力する

ことを特徴とする請求項２に記載の記録媒体。

【請求項５】　前記セキュア記憶手段は、前記使用条件が所定のキー情報を用いて暗号化されて生成された前記ライセンス情報を記憶しており、

前記耐タンパモジュール手段は、前記キー情報を記憶しており、前記キー情報を用いて、前記ライセンス情報を復号して前記使用条件を生成し、生成した使用条件に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する

ことを特徴とする請求項２に記載の記録媒体。

【請求項６】　前記セキュア記憶手段は、前記ライセンス情報の一部分を記憶しており、

前記耐タンパモジュール手段は、さらに、前記ソフトウェアの他の部分を記憶

しており、インストール又はアンインストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報の前記一部分を抽出し、抽出した前記一部分と記憶している前記他の部分とからライセンス情報を生成する

ことを特徴とする請求項２に記載の記録媒体。

【請求項７】　前記セキュア記憶手段が記憶しているライセンス情報は、前記ソフトウェアの使用許可回数であり、

前記耐タンパモジュール手段は、前記使用許可回数が０より大きいか否かを判断し、０より大きいと判断する場合に、前記ソフトウェアの使用が許可されたとみなして、前記許可指示、前記ソフトキー、もしくは前記署名データのうち、少なくとも一つを出力し、さらに、前記使用許可回数から１減じて前記セキュア記憶手段に書き込む

ことを特徴とする請求項２、請求項３、請求項４、請求項５、又は請求項６に記載の記録媒体。

【請求項８】　前記セキュア記憶手段が記憶しているライセンス情報は、前記ソフトウェアの使用許可回数であり、

前記耐タンパモジュール手段は、前記ソフトウエアのアンインストールが許可された場合に、前記許可指示を出力し、さらに、前記使用許可回数を１加算して前記セキュア記憶手段に書き込む

ことを特徴とする請求項２、請求項３、請求項４、請求項５、又は請求項６に記載の記録媒体。

【請求項９】　ソフトウェアを記録している記録媒体から、前記ソフトウェアを取得して内部に記録し、前記ソフトウェアに従って動作する情報処理装置であって、

前記記録媒体は、

ソフトウェアを記憶している通常記憶手段と、

前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、

耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に

基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備え、

前記情報処理装置は、

前記ソフトウェアを記憶するための領域を備える記憶手段と、

前記記録媒体から前記許可指示を取得する取得手段と、

取得した前記許可指示に応じて、前記記録媒体から前記ソフトウェアを取得して前記記憶手段に書き込み、又は前記記憶手段に記憶されている前記ソフトウェアを非活性化する制御手段と

を備えることを特徴とする情報処理装置。

【請求項１０】　前記セキュア記憶手段は、前記ソフトウェアの署名データを含む前記使用条件に係る前記ライセンス情報を記憶しており、

前記耐タンパモジュール手段は、インストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報から前記署名データを抽出し、抽出した前記署名データを出力し、

前記取得手段は、さらに、前記署名データを取得し、

前記制御手段は、取得した前記署名データ及び取得した前記ソフトウェアを用いて、取得した前記ソフトウェアの正当性の検証を行い、又は取得した前記署名データ及び前記記憶手段に記憶している前記ソフトウェアを用いて、前記ソフトウェアの正当性の検証を行い、検証が成功した場合に、取得した前記許可指示に応じて、取得した前記ソフトウェアを書き込み、又は記憶されている前記ソフトウェアを非活性化する

を備えることを特徴とする請求項９に記載の情報処理装置。

【請求項１１】　ソフトウェアを記録している記録媒体であって、

ソフトウェアを記憶している通常記憶手段と、

前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、

耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断し、許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出し、読み出した前記署名データを出力する耐タンパモジュール手段と

を備えることを特徴とする記録媒体。

【請求項１２】　ソフトウェアを記録している記録媒体から前記ソフトウェアを読み出して内部に記憶する情報処理装置であって、

前記記録媒体は、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断し、許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出し、読み出した前記署名データを出力する耐タンパモジュール手段とを備え、

前記情報処理装置は、

前記記録媒体から前記署名データ及び前記ソフトウェアを取得する取得手段と、

取得した前記署名データを用いて、取得した前記ソフトウェアの検証を行い、検証が成功した場合に、取得した前記ソフトウェアを内部に記憶する記憶手段と

を備えることを特徴とする情報処理装置。

【請求項１３】　ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段において用いられる制御方法であって、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する判断ステップと、

可と判断する場合に、前記情報処理装置に対してインストール又はアンインス

トールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える書換ステップと

を含むことを特徴とする制御方法。

【請求項１４】　ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段において用いられる制御プログラムであって、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する判断ステップと、

可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える書換ステップと

を含むことを特徴とする制御プログラム。

【請求項１５】　ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段において用いられる制御プログラムを記録しているコンピュータ読み取り可能なプログラム記録媒体であって、

前記制御プログラムは、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する判断ステップと、

可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応

じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える書換ステップと

を含むことを特徴とする記録媒体。

【請求項１６】　ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段により用いられるインストール方法であって、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断する判断ステップと、

許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出す読出ステップと、

読み出した前記署名データを出力する出力ステップと

を含むことを特徴とするインストール方法。

【請求項１７】　ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段により用いられるインストールプログラムであって、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断する判断ステップと、

許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出す読出ステップと、

読み出した前記署名データを出力する出力ステップと

を含むことを特徴とするインストールプログラム。

【請求項１８】　ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備えるソフトウェア記録媒体における前記耐タ

ンパモジュール手段により用いられるインストールプログラムを記録しているコンピュータ読み取り可能なプログラム記録媒体であって、

前記インストールプログラムは、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断する判断ステップと、

許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出す読出ステップと、

読み出した前記署名データを出力する出力ステップと

を含むことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータソフトウェアのライセンス管理技術に関する。

【０００２】

【従来の技術】

従来よりコンピュータプログラムのライセンスを管理する様々な技術が提案されている。

特許文献１は、記録媒体に記録されているアプリケーションプログラムが無制限にインストールされることを防止し、不正な使用を解消することを目的として、インストール実行に応じてインストール回数を記録媒体の記録再生領域に記録しておき、アプリケーションプログラムを他の記録媒体へインストールする要求があった場合に、記録されている過去のインストール回数を確認し、そのインストール回数が所定回数未満であったときのみ、インストールを実行するインストール制御技術を開示している。

【０００３】

【特許文献１】

特開平１０－２７４２６号公報

また、特許文献２は、ＩＣカードに格納された情報に基づいて、ソフトウェアの不正使用を防止するソフトウェアライセンス管理システムを開示している。前

記管理システムは、ソフトウェア記録媒体と、該ソフトウェアのライセンス管理情報を格納したＩＣカードと、カードリーダライタを接続した情報処理端末機とを具備しており、前記管理システムは、ソフトウェア購入者が個々に保持する前記情報処理端末機のカードリーダライタを介して前記ＩＣカードからライセンス管理情報を読み出す手段と、該ライセンス管理情報に基づいてインストールまたはアンインストールする手段からなり、前記ＩＣカードにインストールした情報処理端末機を特定する情報を記録する。

【０００４】

【特許文献２】

特開２００２－２６８７６４号公報

さらに、特許文献３は、ソフトウェアのライセンス不正利用を抑止することを目的とするソフトウェアコピーガード実現方法を開示している。前記コピーガード実現方法は、揮発性記憶領域と不揮発性記憶領域が内蔵されたカートリッジに着脱可能な記録媒体が挿入され、カートリッジ内の不揮発性記憶領域に格納された認証アルゴリズムと、ソフトウェアのインストールプログラムと、ソフトウェアをインストールするシステム装置固有のシステム情報と、記録媒体が持つソフトウェア固有の情報と、カートリッジアクセス装置とを利用する。カートリッジは、記録媒体が持つソフトウェア固有の情報及び端末装置に固有の端末固有情報を用いて、認証データを生成して内部に記録し、認証データに基づいてソフトウェアの端末装置へのインストールの可否を判断する。

【０００５】

【特許文献３】

特開２００２－１８２７６９号公報

【０００６】

【発明が解決しようとする課題】

しかしながら、第１に、特許文献１により開示されているインストール制御技術によると、記録媒体に記録されているインストール回数によりインストールを実行するか否かを判断するので、無制限にアプリケーションプログラムがインストールされることを防止できるものの、悪意のある第三者が、記録媒体の記録再

生領域に記録されているインストール回数を改竄すれば、無制限にアプリケーションプログラムをインストールすることができるという問題点（課題１）がある。

【０００７】

また、前記インストール制御技術によると、前記記録媒体からインストール回数が、前記記録媒体とインストールの対象となる端末装置との間の通信路上を流れることにより、端末装置に伝達され、端末装置においてインストール回数を受け取り、受け取ったインストール回数を用いて、端末装置が、インストールの可否を判定する。ここで、悪意のある第三者が、前記通信路上において、インストール回数を改竄すれば、上記と同様に、無制限にアプリケーションプログラムをインストールすることができるという問題点（課題２）がある。

【０００８】

さらに、前記インストール制御技術によると、記録媒体上においてアプリケーションプログラムとインストール回数とが対応付けて記録されているので、悪意のある第三者が、記録媒体上におけるアプリケーションプログラムとインストール回数との対応付けを不正に改竄すれば、例えば、安価なプログラムを正規に購入し、購入した安価なプログラムとインストール回数との対応付けを、正規に購入していない高価なプログラムと前記インストール回数との対応付けに変更すれば、前記高価なプログラムを、インストールすることができるという問題点（課題３）がある。

【０００９】

第２に、特許文献２により開示された管理システムによると、該ソフトウェアのライセンス管理情報がＩＣカードに格納されているので、悪意のある第三者によっても、ＩＣカードに格納されているライセンス管理情報の改竄は容易ではない。従って課題１に指摘するような問題点が発生する可能性は低い。

また、前記管理システムによると、前記ＩＣカードからライセンス管理情報が、前記ＩＣカードとインストールの対象となる情報処理端末機との間の通信路上を流れることにより、情報処理端末機に伝達され、情報処理端末機においてライセンス管理情報を受け取り、受け取ったライセンス管理情報を用いて、情報処理

端末機が、インストールの可否を判定する。ここで、悪意のある第三者が、前記通信路上において、ライセンス管理情報を改竄すれば、特許文献１により開示されているインストール制御技術による場合と同様に、無制限にアプリケーションプログラムをインストールすることができるという問題点（課題２）がある。

【００１０】

さらに、前記管理システムによると、ソフトウェア記録媒体とＩＣカードとが対応付けられているので、悪意のある第三者が、例えば、安価なソフトウェアが記録されている第１のソフトウェア記録媒体及び１００台分のライセンス管理情報を記録した第１のＩＣカードと、高価なソフトウェアが記録されている第２のソフトウェア記録媒体及び１台分のライセンス管理情報を記録した第２のＩＣカードとを正規に購入し、第２のソフトウェア記録媒体が第１のＩＣカードに対応付くように、第２のソフトウェア記録媒体を改竄すれば、前記高価なソフトウェアを、インストールすることができるという問題点（課題３）がある。

【００１１】

第３に、特許文献３により開示されたコピーガード実現方法によると、ソフトウェアのインストールの可否を判断するために用いられる認証データがカートリッジ内に記録されているので、悪意のある第三者によっても、カートリッジに記録されている認証データの改竄は容易ではない。従って課題１に指摘するような問題点が発生する可能性は低い。

【００１２】

また、前記コピーガード実現方法によると、悪意のある第三者が、カートリッジアクセス装置とカートリッジの間の通信路上を流れるライセンス関連情報を改竄すれば、特許文献１により開示されているインストール制御技術による場合と同様に、無制限にアプリケーションプログラムをインストールすることができるという問題点（課題２）がある。

【００１３】

さらに、前記コピーガード実現方法によると、悪意のある第三者が、記録媒体とカートリッジとの対応付けを改竄すれば、特許文献２により開示された管理システムの場合と同様に、例えば、正規に購入していない高価なソフトウェアを、

インストールすることができるという問題点（課題３）がある。

本発明は、上記の問題点（課題１～３）を解決し、コンピュータソフトウェアが記録されている記録媒体上の改竄がされにくく、ソフトウェアがインストールされる対象となる端末装置と前記記録媒体との間の通信路における不当な攻撃を避けることができ、またソフトウェアとライセンス情報との対応関係を不正に更新することができない情報処理システム、記録媒体、情報処理装置、制御方法、制御プログラム、インストール方法、インストールプログラム及び記録媒体を提供することを目的とする。

【００１４】

【課題を解決するための手段】

上記目的を達成するために、本発明は、コンピュータソフトウェアを記録している記録媒体である。前記記録媒体は、セキュア記憶領域及び通常記憶領域を含む情報記憶部と、耐タンパモジュール部とを備えている。

通常記憶領域には、コンピュータ命令の実行手順を示すコンピュータソフトウェアが記憶されており、セキュア記憶領域には、前記コンピュータソフトウェアの使用許可数を示すライセンス数と、前記コンピュータソフトウェアの署名データとが対応付けて記録されている。

【００１５】

耐タンパモジュール部は、前記コンピュータソフトウェアのインストール対象となる端末装置との間で、相互に機器認証を行い、相手が正当な装置であることを確認する。

相手が正当な装置があると確認された場合に、耐タンパモジュール部は、端末装置から暗号化端末固有情報を取得する。暗号化端末固有情報は、端末固有情報が暗号化されたものであり、端末固有情報は、前記端末装置に固有の情報である。耐タンパモジュール部は、取得した暗号化端末固有情報を復号して端末固有情報を得、得られた端末固有情報がセキュア記憶領域にすでに記憶されているなら、ソフトウェアの再インストールとみなす。記憶されていないなら、新規インストールとみなし、前記端末固有情報をセキュア記憶領域に書き込む。耐タンパモジュール部は、セキュア記憶領域に記憶されているライセンス数をチェックし、

ライセンス数が所定数以内であれば、コンピュータソフトウェアとコンピュータソフトウェアの署名データとを端末装置へ出力する。

【００１６】

端末装置は、コンピュータソフトウェアと署名データとを受け取り、受け取った署名データを検証し、検証が成功すれば、受け取ったコンピュータソフトウェアを内部にインストールする。

一方、耐タンパモジュール部は、ライセンス数を1だけ減じるように更新する。

【００１７】

【発明の実施の形態】

１．実施の形態１

本発明に係る１個の実施の形態としてのソフトウェア管理システム１０について説明する。

１．１　ソフトウェア管理システム１０の構成

ソフトウェア管理システム１０は、図１に示すように、ソフトウェア書込装置１００、可搬型のメモリカード２００及び情報処理装置３００から構成されている。

【００１８】

ソフトウェア書込装置１００は、ソフトウェア提供者が有しているパーソナルコンピュータ等により構成されるコンピュータシステムであり、ソフトウェア販売店や、ＣＥ（コンシューマエレクトロニクス）機器メーカの顧客サービスセンターにおいて利用される。ソフトウェア書込装置１００は、コンピュータにより実行されるアプリケーションプログラム、前記アプリケーションプログラムの不具合などを修正するためのバグ修正プログラム、前記アプリケーションプログラムの新機能追加のためのバージョンアッププログラムなどのソフトウェアをメモリカード２００に書き込む。前記ソフトウェアは、複数のコンピュータ命令から構成され、これらのコンピュータ命令の実行手順を示すものである。前記ソフトウェアの書き込まれたメモリカード２００は、利用者に有償又は無償で提供される

【００１９】

情報処理装置３００は、利用者が有しているパーソナルコンピュータや家庭電化製品などのＣＥ機器である。利用者により前記ソフトウェアが書き込まれたメモリカード２００が情報処理装置３００に挿入される。情報処理装置３００は、メモリカード２００に書き込まれているソフトウェアを読み出して、内部に記憶、つまりインストールする。情報処理装置３００は、内部に記憶しているソフトウェアに従って動作する。このようにして、利用者は、そのソフトウェアを利用することができる。

【００２０】

また、情報処理装置３００は、内部に記憶しているソフトウェアをアンインストールする。こうして、利用者のそのソフトウェアを非活性化することができる。

１．２　ソフトウェア書込装置１００の構成

ソフトウェア書込装置１００は、図２に示すように、認証部１１１、暗号化部１１２、情報記憶部１１３、制御部１１４及び暗号化部１１８から構成されている。また、ソフトウェア書込装置１００には、入力部１１５及び表示部１１６が接続されている。

【００２１】

ソフトウェア書込装置１００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどから構成されるコンピュータシステムである。また、入力部１１５は、具体的には、キーボードであり、表示部１１６は、ディスプレィユニットである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、ソフトウェア書込装置１００は、その機能を達成する。

【００２２】

なお、図２において、各ブロックは、接続線により他のブロックと接続されている。ただし、一部の接続線を省略している。ここで、各接続線は、信号や情報が伝達される経路を示している。また、暗号化部１１２を示すブロックに接続し

ている複数の接続線のうち、接続線上に鍵マークが付されているものは、暗号化部１１２へ鍵としての情報が伝達される経路を示している。また、他の図面についても同様である。

【００２３】

（１）情報記憶部１１３

情報記憶部１１３は、図２に示すように、ソフトウェア管理テーブル１２１、ソフトウェア１２２、ソフトウェア１２３、・・・をセキュアに記憶している。

ソフトウェア管理テーブル１２１は、ソフトＩＤ、ソフトキー及びインストール回数情報から構成されるソフトウェア管理情報を複数個含むデータテーブルである。

【００２４】

ソフトＩＤは、当該ソフトウェアを識別するための識別番号であり、６４ビット長である。

ソフトキーは、当該ソフトウェアを暗号化する際に用いられる暗号鍵であり、５６ビット長である。

インストール回数情報は、１６ビット長であり、当該ソフトウェアに割り当てられたインストール許可回数である。例えば、インストール回数情報が「１０」である場合に、利用者に対して、当該ソフトウェアを最大１０回までインストールすることが許可される。また、インストール回数情報として「ＦＦＦＦ」（１６進数）が指定された場合には、無制限にインストールが可能であることを示すものとする。ここでは、インストール回数情報は、固定値をとるとしているが、利用者の購入数に応じて可変であるように設定してもよい。

【００２５】

ソフトウェア１２２、ソフトウェア１２３、・・・は、それぞれ、コンピュータプログラムであり、ソフトＩＤにより識別される。

（２）入力部１１５

入力部１１５は、ソフトウェア書込装置１００の操作者からソフトウェアの指定を受け付け、指定を受け付けたソフトウェアを識別するソフトＩＤを情報記憶部１１３から取得し、取得したソフトＩＤを制御部１１４へ出力する。

【００２６】

（３）認証部１１１

メモリカード２００が操作者によりソフトウェア書込装置１００に挿入されると、認証部１１１は、メモリカード２００が有する認証部２１１との間で、チャレンジーレスポンス型の相互の機器認証を行う。

具体的には、認証部１１１は、認証部２１１を認証する。次に、認証部１１１は、認証部２１１により、認証を受ける。

【００２７】

認証部１１１及び認証部２１１の認証が共に成功した場合に、認証部１１１と認証部２１１との間での上記チャレンジーレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいて、相互の認証の都度異なる６４ビット長のセッション鍵を生成し、生成したセッション鍵を認証部２１１との間で秘密に共有する。次に認証部１１１は、生成したセッション鍵を暗号化部１１８へ出力する。

【００２８】

認証部１１１は、両者の認証が成功した場合に、認証の成功を示す認証成功情報を制御部１１４へ出力し、認証が失敗した場合に、認証の失敗を示す認証失敗情報を制御部１１４へ出力する。

なお、チャレンジーレスポンス型の機器認証については、公知であるので、説明を省略する。

【００２９】

（４）制御部１１４

制御部１１４は、入力部１１５からソフトＩＤを受け取る。また、制御部１１４は、認証部１１１から認証成功情報又は認証失敗情報を受け取る。

認証部１１１から認証成功情報を受け取ると、制御部１１４は、暗号化部１１８に対して受け取ったソフトＩＤを出力し、また暗号化部１１８に対してソフトウェア管理情報を暗号化してメモリカード２００へ書き込む旨の暗号化指示を出力する。また、制御部１１４は、暗号化部１１２に対して受け取ったソフトＩＤを出力し、暗号化部１１２に対してソフトウェアを暗号化してメモリカード２００へ書き込む旨の暗号化指示を出力する。

【００３０】

（５）暗号化部１１８

暗号化部１１８は、制御部１１４からソフトＩＤ及び暗号化指示を受け取る。また、暗号化部１１８は、認証部１１１からセッション鍵を受け取る。

制御部１１４からソフトＩＤ及び暗号化指示を受け取ると、暗号化部１１８は、ソフトウェア管理テーブル１２１から、前記ソフトＩＤを含むソフトウェア管理情報を読み出し、認証部１１１から受け取ったセッション鍵を用いて、読み出したソフトウェア管理情報に暗号化アルゴリズムＥ３を施し、暗号化ソフトウェア管理情報を生成する。次に、暗号化部１１８は、生成した暗号化ソフトウェア管理情報をメモリカード２００へ出力する。

【００３１】

（６）暗号化部１１２

暗号化部１１２は、制御部１１４からソフトＩＤ及び暗号化指示を受け取る。

制御部１１４からソフトＩＤ及び暗号化指示を受け取ると、ソフトウェア管理テーブル１２１から前記ソフトＩＤを含むソフトウェア管理情報を読み出し、読み出したソフトウェア管理情報からソフトキーを抽出する。次に、暗号化部１１２は、情報記憶部１１３から受け取ったソフトＩＤにより識別されるソフトウェアを読み出し、抽出したソフトキーを鍵として用いて、読み出したソフトウェアに暗号化アルゴリズムＥ１を施し、暗号化ソフトウェアを生成する。

【００３２】

ここで、暗号化アルゴリズムＥ１は、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）により規定されたものである。

なお、ソフトキーのビット長、暗号化アルゴリズムについては、上記に説明したものに限定されない。

次に、暗号化部１１２は、生成した暗号化ソフトウェアをメモリカード２００へ出力する。

【００３３】

（７）表示部１１６

表示部１１６は、制御部１１４の制御により各種情報を表示する。

１．３　メモリカード２００の構成

メモリカード２００は、図２及び図３に示すように、特別に許可された経路を除いて、外部から読み書きできない耐タンパモジュール部２１０及び情報記憶部２２０から構成されている。耐タンパモジュール部２１０は、認証部２１１、復号部２１２、暗号化部２１３及び判定部２１４から構成され、情報記憶部２２０は、第１記憶領域２２１及び第２記憶領域２２２から構成されている。

【００３４】

ここで、耐タンパモジュール部２１０は、具体的には、耐タンパ性を有する耐タンパハードウェアにより構成されている。なお、耐タンパモジュール部２１０は、耐タンパソフトウェア、又は耐タンパハードウェア及び耐タンパソフトウェアの組み合わせから構成されているとしてもよい。

また、耐タンパモジュール部２１０は、具体的には、マイクロプロセッサ、及びＲＯＭ、ＲＡＭなどのメモリ部から構成され、前記メモリ部には、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、耐タンパモジュール部２１０は、その機能を達成する。

【００３５】

情報記憶部２２０は、具体的には、大容量のフラッシュメモリにより構成されている。

（１）第１記憶領域２２１

第１記憶領域２２１は、特別の許可がなくとも、外部からアクセスすることが許されている領域である。

【００３６】

第１記憶領域２２１は、１個以上の暗号化ソフトウェアを記憶するための領域を備えている。

（２）第２記憶領域２２２

第２記憶領域２２２は、ソフトウェア管理情報テーブル２３１を有している。

ソフトウェア管理情報テーブル２３１は、図４に示すように、複数個のソフトウェア管理情報２４１、２４２、・・・を記憶するための領域を含んでいる。

【００３７】

ソフトウェア管理情報２４１は、この図に示すように、ソフトＩＤ、ソフトキー、インストール回数情報及び複数の装置ＩＤを含む。ソフトＩＤ、ソフトキー及びインストール回数情報については、上述した通りであるので説明を省略する。

装置ＩＤは、ソフトウェアがインストールされる対象となる情報処理装置を一意に識別するための識別番号である。

【００３８】

なお、図４に示すソフトウェア管理情報２４１において、括弧内に表示されている文字列「ＳＩＤ１」、「ＸＹＺ１２３」、「１０」、「＃１」及び「＃２」は、それぞれ、ソフトＩＤ、ソフトキー、インストール回数情報及び２個の装置ＩＤの具体例としての値である。

なお、図４に示すソフトウェア管理情報２４１は、複数の装置ＩＤを含むように示されているが、ソフトウェア書込装置１００からメモリカード２００に、ソフトウェア管理情報が書き込まれる時点においては、まだ、ソフトウェア管理情報２４１は、複数の装置ＩＤを含んでいない。装置ＩＤは、ソフトウェアが情報処理装置にインストールされたときに、ソフトウェア管理情報２４１内に書き込まれる。利用者は、提供されたメモリカードを用いて、初めてソフトウェアをインストールする際には、任意の情報処理装置に、ソフトウェアのインストールを実行することができる。

【００３９】

ソフトウェア管理情報２４２、・・・については、ソフトウェア管理情報２４１と同様であるので、説明を省略する。

（３）認証部２１１

メモリカード２００がソフトウェア書込装置１００に挿入されると、認証部２１１は、ソフトウェア書込装置１００が有する認証部１１１との間で、チャレンジーレスポンス型の相互の機器認証を行う。

【００４０】

具体的には、認証部２１１は、認証部１１１により認証を受ける。次に、認証

部２１１は、認証部１１１の認証を行う。

認証部２１１は、両者の認証が成功した場合に、認証部１１１との間で上記チャレンジーレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいて、相互認証の都度、異なるセッション鍵を生成し、認証部２１１は、生成したセッション鍵を復号部２１２へ出力し、さらに認証の成功を示す第１認証成功情報を判定部２１４へ出力する。一方、認証が失敗した場合に、認証部２１１は、認証の失敗を示す第１認証失敗情報を判定部２１４へ出力する。

【００４１】

また、認証部２１１は、情報処理装置３００が有する認証部３１１との間で、チャレンジーレスポンス型の相互の認証を行う。具体的には、認証部２１１は、認証部３１１により認証を受ける。次に、認証部２１１は、認証部３１１の認証を行う。

両者の認証が成功した場合に、認証部２１１は、認証部３１１との間で上記チャレンジーレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいて、相互の認証の都度、異なるセッション鍵を生成し、認証部３１１との間で生成したセッション鍵を秘密に共有する。認証部２１１は、生成したセッション鍵を復号部２１２及び暗号化部２１３へ出力し、さらに、認証の成功を示す第２認証成功情報を判定部２１４へ出力する。

【００４２】

認証が失敗した場合に認証部２１１は、認証の失敗を示す第２認証失敗情報を判定部２１４へ出力する。メモリカード２００よる以降の処理は中止される。従って、この場合、情報処理装置３００に、メモリカード２００からソフトウェアがインストールされることはない。インストール処理が中止されたことは、メモリカード２００から情報処理装置３００に通知され、情報処理装置３００の利用者に知らされる。

【００４３】

なお、相互の機器認証のプロセスにおけるセッション鍵の共有方法については、公知であるので、説明を省略する。

（４）復号部２１２

復号部２１２は、認証部２１１からセッション鍵を受け取る。

また、復号部２１２は、ソフトウェア書込装置１００から暗号化ソフトウェア管理情報を受け取り、受け取ったセッション鍵を用いて受け取った暗号化ソフトウェア管理情報に復号アルゴリズムＤ３を施してソフトウェア管理情報を生成し、生成したソフトウェア管理情報を判定部２１４へ出力する。

【００４４】

さらに、復号部２１２は、情報処理装置３００の暗号化部３１２から、暗号化区分、暗号化ソフトＩＤ及び暗号化装置ＩＤを受け取り、受け取ったセッション鍵を用いて、受け取った暗号化区分、暗号化ソフトＩＤ及び暗号化装置ＩＤに、復号アルゴリズムＤ３を施して、それぞれ、区分、ソフトＩＤ及び装置ＩＤを生成し、生成した区分、ソフトＩＤ及び装置ＩＤを判定部２１４へ出力する。

【００４５】

ここで、復号アルゴリズムＤ３は、暗号化アルゴリズムＥ３に対応するものであり、暗号化アルゴリズムＥ３を用いて生成された暗号文を、復号するために用いられる。

また、アンインストールの際に、復号部２１２は、暗号化部３１２から暗号化完了情報を受け取り、認証部２１１から受け取ったセッション鍵を用いて、受け取った暗号化完了情報に復号アルゴリズムＤ３を施して、完了情報及び乱数Ｒ’を生成し、生成した完了情報及び乱数Ｒ’を判定部２１４へ出力する。

【００４６】

（５）暗号化部２１３

暗号化部２１３は、認証部２１１からセッション鍵を受け取る。また、暗号化部２１３は、判定部２１４より、ソフトキーを受け取る。次に、暗号化部２１３は、受け取ったセッション鍵を用いて、受け取ったソフトキーに暗号化アルゴリズムＥ４を施して、暗号化ソフトキーを生成する。

【００４７】

ここで、暗号化アルゴリズムＥ４は、ＤＥＳにより規定されたものである。

次に、暗号化部２１３は、生成した暗号化ソフトキーを情報処理装置３００へ出力する。

また、アンインストールの際には、暗号化部２１３は、判定部２１４から、乱数Ｒ及びアンインストール可否情報を受け取り、認証部２１１から受け取ったセッション鍵を用いて、受け取った乱数Ｒ及びアンインストール可否情報に暗号化アルゴリズムＥ４を施して、暗号化アンインストール可否情報を生成し、生成した暗号化アンインストール可否情報を情報処理装置３００へ出力する。

【００４８】

（６）判定部２１４

判定部２１４は、認証部２１１から第１認証成功情報又は第１認証失敗情報を受け取り、また認証部２１１から第２認証成功情報又は第２認証失敗情報を受け取る。

（Ａ）第１認証成功情報を受け取った場合に、判定部２１４は、さらに復号部２１２からソフトウェア管理情報を受け取り、受け取ったソフトウェア管理情報をソフトウェア管理情報テーブル２３１内に追加して書き込む。

【００４９】

（Ｂ）また、第２認証成功情報を受け取った場合に、判定部２１４は、さらに、復号部２１２から区分、ソフトＩＤ及び装置ＩＤを受け取る。

次に、判定部２１４は、受け取った区分がインストールを示すか又はアンインストールを示すかを判断する。

（Ｂ１）インストールを示す場合

受け取った区分がインストールを示すと判断する場合に、判定部２１４は、次に、受け取ったソフトＩＤを含むソフトウェア管理情報をソフトウェア管理情報テーブル２３１から抽出し、抽出したソフトウェア管理情報に、受け取った装置ＩＤが含まれているか否かを判断する。

【００５０】

（ａ１）装置ＩＤが含まれていないと判断する場合には、判定部２１４は、新しい情報処理装置へのインストールの要請であると判断し、次に、前記ソフトウェア管理情報に含まれるインストール回数情報をチェックする。

このとき、（ａ１－１）インストール回数情報が１以上であれば、判定部２１４は、インストールを許可すると判定し、前記復号部２１２より受取った装置Ｉ

Ｄを前記ソフトウェア管理情報に追加して書き込み、前記ソフトウェア管理情報に含まれるインストール回数情報から１を減算して得られる値を、新たにインストール回数情報として、ソフトウェア管理情報テーブル２３１内の前記ソフトウェア管理情報内に上書きする。さらに、判定部２１４は、前記ソフトウェア管理情報に含まれるソフトキーを暗号化部２１３に出力する。

【００５１】

一方、（ａ１－２）前記インストール回数情報のチェックにおいて、インストール回数情報が零であれば、判定部２１４は、インストールを許可しないと判定し、以降の処理を中止する。従って、この場合、情報処理装置３００に、メモリカード２００からソフトウェアがインストールされることはない。インストール処理が中止されたことは、メモリカード２００から情報処理装置３００に通知され、情報処理装置３００は、この旨を表示することにより、利用者に通知する。

【００５２】

（ａ２）装置ＩＤが含まれていると判断する場合には、判定部２１４は、既にインストール済みの情報処理装置への再インストールの要請であると判断し、前記ソフトウェア管理情報に含まれるソフトキーを暗号化部２１３に出力する。

（Ｂ２）アンインストールを示す場合

受け取った区分がアンインストールを示すと判断する場合に、判定部２１４は、さらに、受け取ったソフトＩＤを含むソフトウェア管理情報をソフトウェア管理情報テーブル２３１から抽出し、抽出したソフトウェア管理情報に、復号部２１２から受け取った装置ＩＤが含まれているか否か判断する。

【００５３】

ここで、装置ＩＤが含まれないと判断する場合に、判定部２１４は、アンインストール不可と判定してアンインストール不可を示す８ビット長のアンインストール可否情報を生成する。

一方、装置ＩＤが含まれると判断する場合は、判定部２１４は、アンインストール可と判定してアンインストール可を示す８ビット長のアンインストール可否情報を生成する。

【００５４】

次に、判定部２１４は、５６ビット長の乱数Ｒを生成し、生成した乱数Ｒを保持する。次に、判定部２１４は、生成した乱数Ｒ及びアンインストールの可否を示すアンインストール可否情報を暗号化部２１３へ出力する。

また、判定部２１４は、完了情報及び乱数Ｒ’を受け取り、受け取った乱数Ｒ’と保持している乱数Ｒとが一致するか否かを判断する。ここで、一致しない場合には、アンインストール処理を中止する。一方、一致する場合には、判定部２１４は、さらに、完了情報がアンインストールが完了したことを示しているか否かを判断し、完了情報がアンインストールが完了したことを示していない場合は、以降のアンインストール処理を中止する。

【００５５】

ここで、完了情報がアンインストールが完了したことを示している場合は、判定部２１４は、ソフトウェア管理情報に含まれるインストール回数情報に「１」の値を加算し、得られた値を、新たにインストール回数情報として、ソフトウェア管理テーブル２３１内の前記ソフトウェア管理情報内に上書きする。

（Ｃ）第１認証失敗情報又は第２認証失敗情報を受け取った場合に、判定部２１４は、以降の処理を中止する。

【００５６】

なお、実施の形態１では、判定部２１４は、まずソフトウェア管理テーブルに装置ＩＤが含まれているか否かをチェックし、次に、インストール回数情報のチェックを行うとしているが、これに限定されるものではない。まずインストール回数情報のチェックを行い、次に装置ＩＤのチェックを行うように構成しても良い。

【００５７】

１．４　情報処理装置３００の構成

情報処理装置３００は、図３に示すように、インストール処理部３１０、ソフトウェア格納部３２０、制御部３２１、表示部３２２、入力部３２３、ソフトウェア実行部３２４及び復号部３２５から構成されている。インストール処理部３１０は、さらに、認証部３１１、暗号化部３１２、復号部３１３、復号部３１４、暗号化部３１５、装置ＩＤ格納部３１６、装置固有鍵生成部３１７、ソフトＩ

Ｄ取得部３１８及び乱数格納部３２６から構成されている。

【００５８】

情報処理装置３００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどのメモリ部、キーボード、マウスなどの入力部、ディスプレイユニットなどの表示部から構成されるコンピュータシステムである。前記メモリ部には、インストール処理用のコンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記インストール処理用のコンピュータプログラムに従って動作することにより、情報処理装置３００は、インストール処理の機能を達成する。また、メモリカードから、ソフトウェアがインストールされた暁には、前記マイクロプロセッサが、前記インストールされたソフトウェアに従って動作することにより、情報処理装置は、インストールされたソフトウェアが提供する機能を達成する。

【００５９】

（１）ソフトウェア格納部３２０

ソフトウェア格納部３２０は、具体的には、ハードディスクユニットから構成され、メモリカード２００からインストールされる暗号化ソフトウェアを１個以上記憶する領域を備えている。

（２）装置ＩＤ格納部３１６

装置ＩＤ格納部３１６は、情報処理装置３００に固有の装置ＩＤを、書き換え不可能な形で記憶している。装置ＩＤは、６４ビット長のデータであり、情報処理装置３００を一意に識別する識別情報である。

【００６０】

（３）ソフトＩＤ取得部３１８

ソフトＩＤ取得部３１８は、利用者がインストールを指定したソフトウェアのソフトＩＤを取得する。

ソフトＩＤの取得の具体的な方法としては、例えば、利用者により情報処理装置３００にメモリカード２００が装着された際に、情報処理装置３００が有する表示部３２２は、メモリカード２００内に記憶されている暗号化ソフトウェアの一覧を表示する。入力部３２３は、その一覧からインストールしたいソフトウェ

アの指定を利用者のマウスの操作により、受け付ける。その結果として、ソフトＩＤ取得部３１８は、指定を受け付けたソフトウェアに対応するソフトＩＤを取得する。

【００６１】

（４）認証部３１１

メモリカード２００が利用者により情報処理装置３００に挿入されると、認証部３１１は、メモリカード２００が有する認証部２１１との間で、チャレンジーレスポンス型の相互の機器認証を行う。具体的には、認証部３１１は、認証部２１１を認証する。次に、認証部３１１は、認証部２１１により、認証を受ける。両方の装置の認証が成功した場合にのみ、相互の認証が成功したものと見做される。

【００６２】

両者の認証が成功した場合に、認証部３１１及び認証部２１１との間での上記チャレンジーレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいて、相互の認証の都度、異なるセッション鍵を生成し、生成したセッション鍵を認証部２１１との間で秘密に共有する。

次に、認証部３１１は、生成したセッション鍵を暗号化部３１２及び復号部３１３へ出力する。

【００６３】

認証に失敗した場合に、認証部３１１は、以降の処理を中止する。従って、この場合に、情報処理装置３００が、メモリカード２００からソフトウェアを読み出すことはない。なお、チャレンジーレスポンス型の認証、及びセッション鍵の共有方法については、公知であるので、説明を省略する。

（５）暗号化部３１２

暗号化部３１２は、認証部３１１からセッション鍵を受け取る。

【００６４】

次に、暗号化部３１２は、制御部３２１からソフトウェアのインストール又はアンインストールを示す区分を受け取り、ソフトＩＤ取得部３１８からソフトＩＤを受け取り、装置ＩＤ格納部３１６から装置ＩＤを読み出し、認証部３１１よ

り受け取ったセッション鍵を用いて、前記区分、前記ソフトＩＤ及び前記装置ＩＤに暗号化アルゴリズムＥ３をそれぞれ施して暗号化区分、暗号化ソフトＩＤ及び暗号化装置ＩＤを生成する。

【００６５】

ここで、暗号化アルゴリズムＥ３は、ＤＥＳにより規定されたものである。

次に、暗号化部３１２は、生成した暗号化区分、暗号化ソフトＩＤ及び暗号化装置ＩＤをメモリカード２００へ出力する。

また、アンインストールの際に、暗号化部３１２は、完了情報及び乱数Ｒ’を受け取り、認証部３１１から受け取ったセッション鍵を用いて、受け取った完了情報及び乱数Ｒ’に暗号化アルゴリズムＥ３を施して、暗号化完了情報を生成し、生成した暗号化完了情報を、復号部２１２へ出力する。

【００６６】

（６）復号部３１３

復号部３１３は、認証部３１１からセッション鍵を受け取る。

次に、復号部３１３は、メモリカード２００から、暗号化ソフトキーを受け取り、受け取ったセッション鍵を用いて、受け取った暗号化ソフトキーに復号アルゴリズムＤ４を施して、ソフトキーを生成する。

【００６７】

ここで、復号アルゴリズムＤ４は、ＤＥＳにより規定されたものであり、暗号化アルゴリズムＥ４に対応するものである。復号アルゴリズムＤ４は、暗号化アルゴリズムＥ４を用いて生成された暗号文を復号する。

次に、復号部３１３は、生成したソフトキーを復号部３１４へ出力する。

また、アンインストールの際には、復号部３１３は、メモリカード２００から暗号化アンインストール可否情報を受け取り、認証部３１１から受け取ったセッション鍵を用いて、受け取った暗号化アンインストール可否情報に復号アルゴリズムＤ４を施して、アンインストール可否情報及び乱数Ｒ’を生成し、生成したアンインストール可否情報及び乱数Ｒ’を制御部３２１へ出力する。

【００６８】

（７）復号部３１４

復号部３１４は、メモリカード２００から、前記ソフトＩＤに対応する暗号化ソフトウェアを受け取る。また、復号部３１３からソフトキーを受け取る。

次に、復号部３１４は、受け取ったソフトキーを用いて、受け取った暗号化ソフトウェアに復号アルゴリズムＤ１を施して、ソフトウェアを生成する。

【００６９】

ここで、復号アルゴリズムＤ１は、ＤＥＳにより規定されたものであり、暗号化アルゴリズムＥ１に対応するものである。復号アルゴリズムＤ１は、暗号化アルゴリズムＥ１を用いて生成された暗号文を復号する。

次に、復号部３１４は、生成したソフトウェアを暗号化部３１５へ出力する。

（８）乱数格納部３２６

乱数格納部３２６は、６４ビット長の乱数を格納している。

【００７０】

（９）装置固有鍵生成部３１７

装置固有鍵生成部３１７は、装置ＩＤ格納部３１６から、装置ＩＤを読み出し、次に、乱数格納部３２６から６４ビット長の乱数を読み出し、読み出した乱数をキーとして、読み出した装置ＩＤに暗号化アルゴリズムＦを施して、装置ＩＤに対応する装置固有鍵を秘密に生成し、生成した装置固有鍵を暗号化部３１５及び復号部３２５へ出力する。

【００７１】

ここで暗号化アルゴリズムＦはＤＥＳにより規定されたものである。なお、乱数のビット長、暗号化アルゴリズムについては上記に説明したものに限定されない。

（１０）暗号化部３１５

暗号化部３１５は、装置固有鍵生成部３１７から装置固有鍵を受け取り、復号部３１４からソフトウェアを受け取る。

【００７２】

次に、暗号化部３１５は、受け取った装置固有鍵を用いて、受け取ったソフトウェアに暗号化アルゴリズムＥ２を施して、暗号化ソフトウェアを生成する。

ここで、暗号化アルゴリズムＥ２は、ＤＥＳにより規定されたものである。

次に、暗号化部３１５は、生成した暗号化ソフトウェアをソフトウェア格納部３２０へ書き込む。

【００７３】

（１１）復号部３２５

復号部３２５は、装置固有鍵生成部３１７から装置固有鍵を受け取る。また、復号部３２５は、利用者の指示により、ソフトウェア格納部３２０から暗号化ソフトウェアを読み出す。次に、復号部３２５は、受け取った装置固有鍵を用いて、読み出した暗号化ソフトウェアに復号アルゴリズムＤ２を施して、ソフトウェアを生成する。

【００７４】

ここで、復号アルゴリズムＤ２は、ＤＥＳにより規定されたものであり、暗号化アルゴリズムＥ２に対応するものである。復号アルゴリズムＤ２は、暗号化アルゴリズムＥ２を用いて生成された暗号文を復号する。

次に、復号部３２５は、生成したソフトウェアをソフトウェア実行部３２４へ出力する。

【００７５】

（１２）ソフトウェア実行部３２４

ソフトウェア実行部３２４は、復号部３２５からソフトウェアを受け取り、受け取ったソフトウェアに従って動作する。

（１３）制御部３２１

制御部３２１は、情報処理装置３００を構成する各構成部を制御する。

【００７６】

アンインストールの際には、制御部３２１は、復号部３１３から、アンインストール可否情報及び乱数Ｒ’を受け取り、受け取ったアンインストール可否情報を用いて、アンインストールの可否を判断する。

アンインストールが不可であると判断する場合に、制御部３２１は、アンインストール処理を行わず、アンインストールが未完了であることを示す８ビット長の完了情報を生成する。

【００７７】

アンインストールが可であると判断する場合に、制御部３２１は、ソフトウェア格納部３２０に格納されている暗号化ソフトウェアが実行できないように暗号化ソフトウェアを非活性化処理することにより、該ソフトウェアをアンインストールする。

ここでソフトウェアを非活性化処理するためには、例えば、乱数格納部３２６に格納されている乱数を他の乱数に更新する。

【００７８】

次に、制御部３２１は、ソフトウェアのアンインストールが完了したことを示す８ビット長の完了情報を生成し、生成した完了情報及び乱数Ｒ’を暗号化部３１２へ出力する。

（１４）入力部３２３

入力部３２３は、利用者から入力を受け付ける。具体的には、情報処理装置３００にメモリカード２００が装着されると、入力部３２３は、利用者からソフトウェアのインストール又はアンインストールを示す区分を受け付け、受け付けた区分を制御部３２１を介して、暗号化部３１２へ出力する。

【００７９】

インストールを示す区分を受け付けた場合には、入力部３２３は、さらに、利用者からインストールするソフトウェアの指定を受け付ける。一方、アンインストールを示す区分を受け付けた場合には、入力部３２３は、利用者からアンインストールする暗号化ソフトウェアの指定を受け付ける。

（１５）表示部３２２

表示部３２２は、制御部３２１の制御により、各種情報を表示する。具体的には、入力部３２３がインストールを示す区分を受け付けた場合には、表示部３２２は、メモリカード２００に記憶されているソフトウェアの一覧を表示する。一方、入力部３２３がアンインストールを示す区分を受け付けた場合には、表示部３２２は、情報処理装置３００のソフトウェア格納部３２０に格納されている暗号化ソフトウェアの一覧を表示する。

【００８０】

１．５　ソフトウェア管理システム１０の動作

利用者が情報処理装置３００にメモリカード２００を装着した後に、メモリカード２００に記憶されているソフトウェアを情報処理装置３００へインストールする場合及び情報処理装置３００に既にインストールされている暗号化ソフトウェアをアンインストールする場合のソフトウェア管理システム１０の動作について、図５～９に示すフローチャートを用いて説明する。

【００８１】

情報処理装置３００にメモリカード２００が装着されると、入力部３２３は、利用者からソフトウェアのインストール又はアンインストールを示す区分を受け付け、受け付けた区分を制御部３２１を介して、暗号化部３１２へ出力し、入力部３２３がインストールを示す区分を受け付けた場合には、表示部３２２は、メモリカード２００に記憶されているソフトウェアの一覧を表示し、入力部３２３は、利用者からインストールするソフトウェアの指定を受け付け、入力部３２３がアンインストールを示す区分を受け付けた場合には、表示部３２２は、情報処理装置３００のソフトウェア格納部３２０に格納されている暗号化ソフトウェアの一覧を表示し、入力部３２３は、利用者からアンインストールする暗号化ソフトウェアの指定を受け付ける（ステップＳ１００）。

【００８２】

情報処理装置３００は、ソフトウェア又は暗号化ソフトウェアの指定を受け付けると、情報処理装置３００が有する認証部３１１とメモリカード２００が有する認証部２１１との間で、相互に認証を行う（ステップＳ１０１、ステップＳ１０２）。

認証に成功すると（ステップＳ１０４）、暗号化部３１２は、認証部３１１よりセッション鍵を受け取り、ソフトＩＤ取得部３１８よりソフトＩＤを受け取り、装置ＩＤ格納部より装置ＩＤを読み出し、受け取ったセッション鍵を用いて、区分、ソフトＩＤ及び装置ＩＤを暗号化して暗号化区分、暗号化ソフトＩＤ及び暗号化装置ＩＤを生成し（ステップＳ１０５）、生成した暗号化区分、暗号化ソフトＩＤ及び暗号化装置ＩＤをメモリカード２００に送信する（ステップＳ１０６）。

【００８３】

認証に成功すると（ステップＳ１０３）、復号部２１２は、認証部２１１よりセッション鍵を受け取り、受け取ったセッション鍵を用いて、情報処理装置３００より受信した暗号化区分、暗号化ソフトＩＤ及び暗号化装置ＩＤを復号し、生成した区分、ソフトＩＤ及び装置ＩＤを判定部２１４に送る（ステップＳ１０７）。

【００８４】

認証に失敗すると（ステップＳ１０３又はＳ１０４）、メモリカード２００又は情報処理装置３００は、以降の処理を中止する。

次に、判定部２１４は、第２記憶領域２２２から、前記生成されたソフトＩＤに対応するソフトウェア管理情報を読出し（ステップＳ１０８）、生成された区分がソフトウェアのインストール又はアンインストールのいずれを示すかを判断する（ステップＳ１０９）。

【００８５】

（インストール時の処理）

区分がソフトウェアのインストールを示すと判断する場合に（ステップＳ１０９）、判定部２１４は、読み出したソフトウェア管理情報に基づいて、インストールを許可するか否かを判定する（ステップＳ１１０）。なおステップＳ１１０の詳細は後述する。

【００８６】

インストールを許可しないと判定した場合に（ステップＳ１１０）、判定部２１４は、不許可を示す不許可メッセージを情報処理装置３００に送信し（ステップＳ１２０）、その後、メモリカード２００は、処理を中止する。

メモリカード２００から前記不許可メッセージを受け取ると（ステップＳ１２１）、制御部３２１は、表示部３２２に対して前記不許可メッセージを表示するように制御し、表示部３２２は、前記不許可メッセージを表示し（ステップＳ１２２）、その後、情報処理装置３００は、処理を中止する。

【００８７】

インストールを許可すると判定した場合に（ステップＳ１１０）、判定部２１４は、ソフト管理情報に含まれるソフトキーを暗号化部２１３に送り、暗号化部

２１３は、ソフトキーを、認証部２１１より受け取ったセッション鍵を用いて暗号化して暗号化ソフトキーを生成し（ステップＳ１１１）、生成した暗号化ソフトキーを情報処理装置３００に送信し（ステップＳ１１２）、制御部３２１が前記不許可メッセージを受け取っていない場合に（ステップＳ１２１）、復号部３１３は、メモリカード２００から受け取った暗号化ソフトキーを、認証部３１１より受け取ったセッション鍵を用いて復号する（ステップＳ１１３）。

【００８８】

また、第１記憶領域２２１から暗号化ソフトウェアが読み出され（ステップＳ１１４）、読み出された暗号化ソフトウェアが情報処理装置３００へ送信される（ステップＳ１１５）。復号部３１４は、復号部３１３から受取った復号されたソフトキーを用いて、暗号化ソフトウェアを復号し（ステップＳ１１６）、復号されたソフトウェアを暗号化部３１５へ送り、装置固有鍵生成部３１７は、装置ＩＤ格納部３１６より装置ＩＤを読み出し、読み出した装置ＩＤを用いて装置固有鍵を生成し（ステップＳ１１７）、暗号化部３１５は、復号部３１４より受け取ったソフトウェアを、装置固有鍵生成部３１７より受け取った装置固有鍵を用いて暗号化して暗号化ソフトウェアを生成し（ステップＳ１１８）、暗号化部３１５は、生成した暗号化ソフトウェアをソフトウェア格納部３２０に書き込むことにより、インストールする（ステップＳ１１９）。

【００８９】

以上のようにして、暗号化ソフトウェアのインストールが完了する。

（アンインストール時の処理）

区分がソフトウェアのアンインストールを示すと判断する場合に（ステップＳ１０９）、さらに、判定部２１４は、復号部２１２から受け取った装置ＩＤが、第２記憶領域２２２から読み出したソフトウェア管理情報に含まれるかどうかを判断し、装置ＩＤが含まれない場合は（ステップＳ２０１）、アンインストール不可と判定してアンインストール不可を示す８ビット長のアンインストール可否情報を生成する（ステップＳ２０３）。一方、装置ＩＤが含まれる場合は（ステップＳ２０１）、判定部２１４は、アンインストール可と判定してアンインストール可を示す８ビット長のアンインストール可否情報を生成する（ステップＳ２

０２）。

【００９０】

次に、判定部２１４は、５６ビット長の乱数Ｒを生成し、生成した乱数Ｒを保持し（ステップＳ２０４）、生成した乱数Ｒ及びアンインストールの可否を示すアンインストール可否情報を暗号化部２１３へ出力し、暗号化部２１３は、乱数Ｒ及びアンインストール可否情報を受け取り、認証部２１１から受け取ったセッション鍵を用いて、受け取った乱数Ｒ及びアンインストール可否情報に暗号化アルゴリズムＥ４を施して、暗号化アンインストール可否情報を生成し（ステップＳ２０５）、生成した暗号化アンインストール可否情報を情報処理装置３００へ出力する（ステップＳ２０６）。

【００９１】

復号部３１３は、メモリカード２００から暗号化アンインストール可否情報を受け取り（ステップＳ２０６）、認証部３１１から受け取ったセッション鍵を用いて、受け取った暗号化アンインストール可否情報に復号アルゴリズムＤ４を施して、アンインストール可否情報及び乱数Ｒ’を生成し、生成したアンインストール可否情報及び乱数Ｒ’を制御部３２１へ出力する（ステップＳ２０７）。

【００９２】

次に、制御部３２１は、アンインストール可否情報及び乱数Ｒ’を受け取り、受け取ったアンインストール可否情報を用いて、アンインストールの可否を判断し、アンインストールが不可であると判断する場合に（ステップＳ２０８）、アンインストール処理を行わず、アンインストールが未完了であることを示す８ビット長の完了情報を生成し（ステップＳ２１１）、次に、ステップＳ２１２へ制御を移す。

【００９３】

アンインストールが可であると判断する場合に（ステップＳ２０８）、制御部３２１は、ソフトウェア格納部３２０に格納されている暗号化ソフトウェアが実行できないように暗号化ソフトウェアを非活性化処理することにより、該ソフトウェアをアンインストールする。ここでソフトウェアを非活性化処理するためには、例えば、乱数格納部３２６に格納されている乱数を他の乱数に更新すればよ

い（ステップＳ２０９）。次に、制御部３２１は、ソフトウェアのアンインストールが完了したことを示す８ビット長の完了情報を生成する（ステップＳ２１０）。

【００９４】

次に、制御部３２１は、完了情報及び乱数Ｒ’を暗号化部３１２へ出力し、暗号化部３１２は、完了情報及び乱数Ｒ’を受け取り、認証部３１１から受け取ったセッション鍵を用いて、受け取った完了情報及び乱数Ｒ’に暗号化アルゴリズムＥ３を施して、暗号化完了情報を生成し（ステップＳ２１２）、生成した暗号化完了情報を、復号部２１２へ出力する（ステップＳ２１３）。

【００９５】

復号部２１２は、暗号化部３１２から暗号化完了情報を受け取り（ステップＳ２１３）、認証部２１１から受け取ったセッション鍵を用いて、受け取った暗号化完了情報に復号アルゴリズムＤ３を施して、完了情報及び乱数Ｒ’を生成し、生成した完了情報及び乱数Ｒ’を判定部２１４へ出力する（ステップＳ２１４）。

【００９６】

次に、判定部２１４は、完了情報及び乱数Ｒ’を受け取り、受け取った乱数Ｒ’と保持している乱数Ｒとが一致するか否かを判断し、一致しない場合には（ステップＳ２１５）、アンインストール処理を中止する。

一致する場合には（ステップＳ２１５）、判定部２１４は、さらに、完了情報がアンインストールが完了したことを示しているか否かを判断し、完了情報がアンインストールが完了したことを示していない場合は（ステップＳ２１６）、以降のアンインストール処理を中止する。

【００９７】

一方、完了情報がアンインストールが完了したことを示している場合は、（ステップＳ２１６）、判定部２１４は、ソフトウェア管理情報に含まれるインストール回数情報に「１」の値を加算し、得られた値を、新たにインストール回数情報として、ソフトウェア管理テーブル２３１内の前記ソフトウェア管理情報内に上書きする（ステップＳ２１７）。

【００９８】

このようにして、アンインストールが完了する。

以上で説明したアンインストールの手順を利用すれば、例えば、利用者が、暗号化ソフトウェアをインストールしていたハードディスクユニットを、新規のハードディスクユニットに交換したいような場合に、メモリカードに記録されているインストール回数情報が、例え「０」を示している場合であっても、アンインストールを実行することにより新規のハードディスクユニットに新たにインストールすることが可能となる。

【００９９】

なお、複数の暗号化ソフトウェアがソフトウェア格納部３２０にインストールされている場合は、前記ステップＳ２０９において、前記乱数格納部３２６に格納されている乱数を更新する前に、アンインストール対象の暗号化ソフトウェア以外の暗号化ソフトウェアに対して、復号部３２５で、更新前の乱数より生成される装置固有鍵を用いて復号してソフトウェアを生成し、生成したソフトウェアを、暗号化部３１５で更新後の乱数より生成される装置固有鍵を用いて、再び暗号化して再暗号化ソフトウェアを生成し、生成した再暗号化ソフトウェアをソフトウェア格納部３２０に格納すればよい（ステップＳ２０９ａ）。

【０１００】

（ステップ１１０の詳細の動作）

次に、判定部２１４における前記ステップ１１０の詳細の動作について、図９に示すフローチャートを用いて説明する。

判定部２１４は、復号部２１２より受け取った装置ＩＤが、第２記憶領域２２２より受取ったソフトウェア管理情報に含まれるかどうかチェックし（ステップＳ１５１）、装置ＩＤが含まれない場合は（ステップＳ１５１）、新しい情報処理装置へのインストールの要請と判断し、ソフトウェア管理情報に含まれるインストール回数をチェックし（ステップＳ１５３）、１以上であれば（ステップＳ１５３）インストール可と判定する。このとき、前記第２記憶領域２２２より読み出したソフトウェア管理情報に、前記復号部２１２より受け取った装置ＩＤを追加して書き込むとともに、インストール回数を１減算した値に更新したソフト

ウェア管理情報を第２記憶領域２２２に書き込む（ステップＳ１５５）。インストール回数が零であれば（ステップＳ１５３）、インストール不可と判定する。また、前記ステップ１５１において、装置ＩＤが含まれる場合は（ステップＳ１５１）、既にインストール済みの情報処理装置への再インストールの要請と判断し、インストール可と判定する。

【０１０１】

なお、ソフトウェア管理情報は、インストール期間情報を含むとしてもよい。ここで、インストール期間情報は、６４ビット長であり、利用者に対して、当該ソフトウェア管理情報に対応するソフトウェアをインストールすることができる期間を制限するものであり、インストール期間の開始日時を示すインストール許可開始日時と、インストール期間の終了日時を示すインストール許可終了日時とから構成される。利用者に対して、インストール許可開始日時からインストール許可終了日時までの期間内においてのみ、当該ソフトウェアのインストールが許可される。この期間内であれば、利用者は、当該ソフトウェアを何回でもインストールすることができる。ここで、インストール期間情報とインストール回数情報の両方が指定されている場合には、許可されている期間が終了するか、インストール回数までインストールした後には、ソフトウェアをインストールすることはできないものとする。

【０１０２】

１．６　その他の例

ソフトウェア管理システム１０は、以下のように構成してもよい。

(1) 実施の形態１においては、ソフトウェア書込装置１００は、パーソナルコンピュータ等で構成されるコンピュータシステムとしているが、この構成に限定されるものではない。例えば、ソフトウェア書込装置１００は、ＫＩＯＳＫ端末により構成されるとしても良い。

【０１０３】

（２）実施の形態１では、ソフトウェアの書き込まれたメモリカード２００は、利用者に提供されるとしているが、この構成に限定されるものではない。

ソフトウェアの書き込まれたメモリカード２００は、ソフトウェア販売店やＣ

Ｅ機器メーカの顧客サービスセンターのサービスマンに提供され、このサービスマンにより、利用者の情報処理装置にメモリカード２００が挿入されるとしても良い。

【０１０４】

（３）実施の形態１では、ソフトウェア書込装置１００がメモリカード２００にソフトウェア管理情報を書き込む時点においては、ソフトウェア管理情報２４１は、装置ＩＤを含まないとしているが、この構成に限定されるものではない。

ソフトウェア書込装置１００がメモリカード２００にソフトウェア管理情報を書き込む時点において、ソフトウェア管理情報２４１は、装置ＩＤを含んでいるとしても良い。

【０１０５】

このように構成することにより、利用者が提供されたメモリカードを用いて初めてソフトウェアをインストールする際に、ソフトウェア提供者は、利用者に対して、ソフトウェアをインストールする情報処理装置を限定できる。

（４）実施の形態１では、ソフトウェアをインストールする際に、復号部３１４は、ソフトキーを用いて、メモリカード２００から受け取った暗号化ソフトウェアを復号し（ステップＳ１１６）、暗号化部３１５は、装置固有鍵を用いて、復号されたソフトウェアを暗号化し（ステップＳ１１７～Ｓ１１８）、生成した暗号化ソフトウェアをソフトウェア格納部３２０に書き込むことによりソフトウェアをインストールする（ステップＳ１１９）としているが、この構成に限定されるものではない。

【０１０６】

装置固有鍵生成部３１７は、装置固有鍵を生成し（ステップＳ１１７）、暗号化部３１５は、生成された装置固有鍵を用いて、復号部３１３から受け取ったソフトキーを暗号化して暗号化ソフトキーを生成し（ステップＳ１１８’）、生成した暗号化ソフトキーと、メモリカード２００から受け取った暗号化ソフトウェアをソフトウェア格納部３２０に書き込むことによりインストールする（ステップＳ１１９’）ように構成にしても良い。

【０１０７】

このとき、情報処理装置３００は、さらに復号部３２７（図示していない）を備え、ソフトウェアの実行時には、復号部３２５は、受け取った装置固有鍵を用いて、暗号化ソフトキーを復号してソフトキーを生成し、生成したソフトキーを復号部３２７へ出力し、復号部３２７は、復号部３２５からソフトキーを受け取り、受け取ったソフトキーを用いて、暗号化ソフトウェアを復号してソフトウェアを生成し、生成したソフトウェアをソフトウェア実行部３２４へ出力する。ソフトウェア実行部３２４は、復号部３２７からソフトウェアを受け取り、受け取ったソフトウェアに従って、ソフトウェア実行部３２４は、動作する。

【０１０８】

（５）実施の形態１では、インストール時及びソフトウェア実行時において、装置固有鍵生成部３１７は、乱数格納部３２６から６４ビット長の乱数を読出すものとし、アンインストール時において、乱数格納部３２６の前記乱数を更新するとしているが、この構成に限定されるものではない。

乱数格納部３２６は、インストールするソフトウェアに対応付けて、６４ビット長の乱数を記憶しており、インストール時及びソフトウェア実行時において、乱数格納部３２６から、インストールするソフトウェアに対応する６４ビット長の乱数を読み出すものとし、アンインストール時において、乱数格納部３２６の前記ソフトウェアに対応する乱数を更新する構成としても良い。

【０１０９】

この構成により、前記ステップＳ２０９において、複数の暗号化ソフトウェアがソフトウェア格納部３２０にインストールされている場合において、実施の形態１で必要であった暗号化ソフトウェアの復号、再暗号化処理（ステップＳ２０９ａ）は不要となる。

（６）実施の形態１では、認証の方法としてチャレンジーレスポンス型の認証を利用し、セッション鍵の共有方法として、チャレンジーレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいてセッション鍵を生成することにより行うものとしているが、この構成に限定されるものではない。

【０１１０】

例えば認証の方法として、デジタル署名を利用する方法を利用し、セッション

鍵の共有方法としては、ディフィーヘルマン（ＤＨ）型鍵共有方法を利用しても良い。

デジタル署名を利用する認証方法については、「現代暗号理論」（池野信一、小山謙二共著、電子情報通信学会）、Ｐ８３，５．３，（２）に、また、ＤＨ型鍵共有方法については、同Ｐ１７５に詳細に説明されている。

【０１１１】

（７）実施の形態１では、ソフトウェアをソフトウェア書込装置がメモリカードに書き込む際に、ソフトキーは、予めソフトウェア管理情報に含まれるものとし、暗号化部１１２により、ソフトウェア管理テーブル１２１から、前記ソフトＩＤを含むソフトウェア管理情報を読み出し、読み出したソフトウェア管理情報からソフトキーを抽出するものとしたが、この構成に限定されるものではない。

【０１１２】

例えば、ソフトキーは、ソフトウェア管理情報に含まれないものとし、暗号化部１１２は、ソフトウェア管理テーブル１２１から、前記ソフトＩＤを含むソフトウェア管理情報を読み出すとともに、ソフトキーを生成するものとしても良い。

（８）実施の形態１では、アンインストール処理において、アンインストール可否情報と、完了情報をそれぞれ８ビットとし、乱数Ｒを５６ビットとしたがこれらのビット長に限定されるものではない。

【０１１３】

（９）実施の形態１では、アンインストール処理のステップＳ２１２において、セッション鍵を用いて、完了情報及び乱数Ｒ’に暗号化アルゴリズムＥ３を施すとしたが、この構成に限定されるものではない。

例えば、完了情報、及び、乱数Ｒ’のビット反転値（Ｒ”）に、暗号化アルゴリズムＥ３を施すとしてもよい。この場合、ステップＳ２１５においては、受け取った乱数Ｒ”と、保持している乱数Ｒのビット反転値が一致するか否かを判断するものとする。

【０１１４】

（１０）実施の形態１では、ソフトウェアは、コンピュータプログラムなどで

あるとしているが、コンピュータプログラムの動作に付随するデータであっても良い。

（１１）実施の形態１のソフトウェア管理テーブルに、機種ＩＤ（グループＩＤ）を含める構成としても良い。ここで、機種ＩＤ（グループＩＤ）は、情報処理装置の種類を識別する識別情報である。また、同一の種類の情報処理装置とは、例えば、同一の処理性能を有するマイクロプロセッサを内蔵するもの、同一の容量のハードディスクを内蔵するもの、同一の容量のメモリを内蔵するもの、同一メーカにより製造されたものなどを言う。

【０１１５】

この場合、情報処理装置は、自身の種類を識別する機種ＩＤ（グループＩＤ）を備え、メモリカードは、機種ＩＤ（グループＩＤ）に基づいて、同一機種（同一グループ）へのインストール、アンインストールの判定を行う。この構成によりインストールを特定機種の情報処理装置に限定することも可能である

（１２）実施の形態１のソフトウェア管理テーブルに、ソフトウェアのバージョン情報を含める構成としても良い。

【０１１６】

この場合、情報処理装置において、インストール対象のソフトＩＤとともに、バージョン情報を受け付け、メモリカードでは、ソフトＩＤとともに、バージョン情報に基づいて、インストールやアンインストールの可否の判定や、該バージョンのソフトウェアのインストールやアンインストールを行う。

（１３）実施の形態１では、メモリカードの第１記憶領域に暗号化ソフトウェアを記憶する構成としたが、これに限定されるものではない。

【０１１７】

暗号化ソフトウェアを、別途、通信回線や、別の記録媒体を介して、情報処理装置が取得する構成としても良い。

２．変形例（１）

実施の形態１の変形例としてのソフトウェア管理システム１０ｂ（図示していない）について説明する。

【０１１８】

ソフトウェア管理システム１０ｂは、ソフトウェア書込装置１００ｂ、可搬型のメモリカード２００ｂ及び情報処理装置３００ｂから構成されている。ソフトウェア書込装置１００ｂ、メモリカード２００ｂ及び情報処理装置３００ｂは、それぞれソフトウェア書込装置１００、メモリカード２００及び情報処理装置３００と同様の構成を有している。

【０１１９】

ここでは、ソフトウェア書込装置１００、メモリカード２００及び情報処理装置３００との相違点を中心として、ソフトウェア書込装置１００ｂ、メモリカード２００ｂ及び情報処理装置３００ｂについて説明する。

２．１　ソフトウェア書込装置１００ｂの構成

ソフトウェア書込装置１００ｂは、図１０に示すように、認証部１１１、暗号化部１１２、情報記憶部１１３、制御部１１４、署名生成部１１７及び入出力部１１８から構成されている。また、ソフトウェア書込装置１００ｂには、入力部１１５及び表示部１１６が接続されている。

【０１２０】

このように、ソフトウェア書込装置１００ｂは、ソフトウェア書込装置１００と同様の構成を有しており、ソフトウェア書込装置１００ｂは、さらに、署名生成部１１７を備えている点において、ソフトウェア書込装置１００と相違する。

（１）署名生成部１１７

署名生成部１１７は、暗号化部１１２から暗号化ソフトウェアを受け取る。暗号化ソフトウェアを受け取ると、署名生成部１１７は、受け取った暗号化ソフトウェアに、デジタル署名生成アルゴリズムＳＩＧを施して、ソフト署名データを生成する。

【０１２１】

ここで、デジタル署名生成アルゴリズムＳＩＧは、１６０ビット長の楕円曲線暗号によるデジタル署名の生成法に基づくものであり、ソフト署名データは、３２０ビット長である。なお、楕円曲線暗号については、「暗号理論の基礎」（Ｄｏｕｇｌａｓ　Ｒ．Ｓｔｉｏｎｓｏｎ著、共立出版株式会社）に詳細に説明されている。

【０１２２】

次に、署名生成部１１７は、生成したソフト署名データをメモリカード２００ｂの判定部２１４へ出力する。

２．２　メモリカード２００ｂの構成

メモリカード２００ｂは、図１０及び図１２に示すように、耐タンパモジュール部２１０及び情報記憶部２２０から構成されている。耐タンパモジュール部２１０及び情報記憶部２２０は、メモリカード２００が有する耐タンパモジュール部２１０及び情報記憶部２２０と同様の構成を有している。

【０１２３】

ここでは、メモリカード２００との相違点を中心として説明する。

（１）判定部２１４

判定部２１４は、認証部２１１から第１認証成功情報を受け取ると、さらに、ソフト署名データを受け取る。次に、判定部２１４は、受け取ったソフト署名データを、受け取ったソフトウェア管理情報内に書き込み、ソフト署名データを含むソフトウェア管理情報をソフトウェア管理情報テーブル２３１内に追加して書き込む。

【０１２４】

ソフト署名データが書き込まれたソフトウェア管理情報の一例を図１１に示す。この図に示すソフトウェア管理情報２４１ｂは、ソフトＩＤ、ソフトキー、インストール回数情報、ソフト署名データ及び複数の装置ＩＤを含む。

なお、図１１に示すソフトウェア管理情報２４１ｂは、複数の装置ＩＤを含むように構成されているが、ソフトウェア書込装置１００からメモリカード２００に、ソフトウェア管理情報が書き込まれる時点においては、まだ、ソフトウェア管理情報２４１ｂは、複数の装置ＩＤを含んでいないものとする。

【０１２５】

判定部２１４が第２認証成功情報を受け取った場合であって、インストールを許可すると判定したときに、受け取ったソフト署名データを情報処理装置３００ｂへ出力する。

２．３　情報処理装置３００ｂの構成

情報処理装置３００ｂは、図１２に示すように、インストール処理部３１０、ソフトウェア格納部３２０、制御部３２１、表示部３２２、入力部３２３、ソフトウェア実行部３２４及び復号部３２５から構成されている。インストール処理部３１０は、さらに、認証部３１１、暗号化部３１２、復号部３１３、復号部３１４、暗号化部３１５、装置ＩＤ格納部３１６、装置固有鍵生成部３１７、ソフトＩＤ取得部３１８及び署名検証部３１９から構成されている。

【０１２６】

このように、情報処理装置３００ｂは、情報処理装置３００と同様の構成を有しており、さらに署名検証部３１９を備えている点において、情報処理装置３００と異なる。

（１）署名検証部３１９

署名検証部３１９は、メモリカード２００ｂの判定部２１４からソフトウェア管理情報に含まれるソフト署名データを受け取る。また、署名検証部３１９は、メモリカード２００ｂの第１記憶領域２２１から暗号化ソフトウェアを読み出す。

【０１２７】

次に、署名検証部３１９は、受け取ったソフト署名データ及び読み出した暗号化ソフトウェアに、デジタル署名検証アルゴリズムＶＲＦを施し、検証成功を示す検証成功情報、又は検証失敗を示す検証失敗情報を生成する。

ここで、デジタル署名検証アルゴリズムＶＲＦは、楕円暗号によるデジタル署名の検証法に基づくものである。

【０１２８】

次に、署名検証部３１９は、検証成功情報又は検証失敗情報を復号部３１４へ出力する。

（２）復号部３１４

復号部３１４は、署名検証部３１９から検証成功情報又は検証失敗情報を受け取る。

【０１２９】

検証失敗情報を受け取ると、復号部３１４は、以降の復号処理を中止する。

検証成功情報を受け取ると、復号部３１４は、暗号化ソフトウェアの復号を継続して行う。

２．４　その他の例

（１）変形例（１）において、署名生成部１１７は、暗号化ソフトウェアにデジタル署名生成アルゴリズムＳＩＧを施してソフト署名データを生成するとしているが、この構成には限定されない。

【０１３０】

署名生成部１１７は、暗号化ソフトウェアとソフトキーとインストール回数情報とにデジタル署名生成アルゴリズムＳＩＧを施してソフト署名データを生成するとしてもよい。

この場合、ソフトウェアのインストール時に、暗号化部２１３は、セッション鍵を用いて、ソフトキー及びインストール回数情報を暗号化して暗号化情報を生成し、生成した暗号化情報を情報処理装置３００ｂへ送信する。情報処理装置３００ｂの復号部３１３は、セッション鍵を用いて、受け取った暗号化情報を復号して、ソフトキー及びインストール回数情報を生成し、署名検証部３１９は、ソフト署名データ、暗号化ソフトウェア、生成されたソフトキー及び生成されたインストール回数情報に、署名検証アルゴリズムＶＲＦを施して、ソフト署名データを検証するものとする。

【０１３１】

また、署名生成部１１７は、ソフトウェアにデジタル署名アルゴリズムＳＩＧを施してソフト署名データを生成するとしても良い。

この場合、インストール時に、署名検証部３１９は、ソフト署名データと、前記ソフトウェアに、署名検証アルゴリズムＶＲＦを施して、ソフト署名データを検証するものとする。なお、この場合、メモリカード２００ｂの第１記憶領域２２１には、暗号化されていないソフトウェアが書き込まれる。

【０１３２】

３．変形例（２）

ソフトウェア管理システム１０ｂの変形例としてのソフトウェア管理システム１０ｃ（図示していない）について説明する。

ソフトウェア管理システム１０ｃは、ソフトウェア書込装置１００ｃ（図示していない）、可搬型のメモリカード２００ｃ及び情報処理装置３００ｃから構成されている。ソフトウェア書込装置１００ｃは、ソフトウェア書込装置１００ｂと同一の構成を有している。メモリカード２００ｃ及び情報処理装置３００ｃは、それぞれメモリカード２００ｂ及び情報処理装置３００ｂと同様の構成を有している。

【０１３３】

ここでは、メモリカード２００ｂ及び情報処理装置３００ｂとの相違点を中心として、メモリカード２００ｃ及び情報処理装置３００ｃについて説明する。

３．１　メモリカード２００ｃの構成

メモリカード２００ｃは、図１３に示すように、耐タンパモジュール部２１０及び情報記憶部２２０から構成されている。耐タンパモジュール部２１０及び情報記憶部２２０は、メモリカード２００ｂが有する耐タンパモジュール部２１０及び情報記憶部２２０と同様の構成を有している。

【０１３４】

ここでは、メモリカード２００ｂとの相違点を中心として説明する。

耐タンパモジュール部２１０は、認証部２１１、復号部２１２、暗号化部２１３及び判定部２１４、復号部２１５、暗号化部２１６及びキー情報記憶部２１７から構成されている。このように、耐タンパモジュール部２１０は、さらに、復号部２１５、暗号化部２１６及びキー情報記憶部２１７を備える点において、メモリカード２００ｂの耐タンパモジュール部２１０と相違する。

【０１３５】

（１）判定部２１４

判定部２１４は、認証部２１１から第１認証成功情報を受け取ると、さらに、ソフト署名データを受け取る。次に、判定部２１４は、受け取ったソフト署名データを、受け取ったソフトウェア管理情報内に書き込み、次に、ソフト署名データを含むソフトウェア管理情報を暗号化部２１６へ出力する。

【０１３６】

ソフト署名データが書き込まれたソフトウェア管理情報の一例は、図１１に示

す通りである。

また、判定部２１４は、復号部２１５からソフトウェア管理情報を受け取る。

（２）キー情報記憶部２１７

キー情報記憶部２１７は、キー情報を記憶している。キー情報は、５６ビット長のデータであり、ソフトウェア管理情報を暗号化又は復号するために用いられる。

【０１３７】

（３）暗号化部２１６

暗号化部２１６は、判定部２１４からソフトウェア管理情報を受け取り、キー情報記憶部２１７からキー情報を読み出す。

次に、暗号化部２１６は、読み出したキー情報を用いて、受け取ったソフトウェア管理情報に暗号化アルゴリズムＥ５を施して、暗号化ソフトウェア管理情報を生成し、生成した暗号化ソフトウェア管理情報を第２記憶領域２２２が有する暗号化ソフトウェア管理情報テーブル２３１ｃに書き込む。

【０１３８】

ここで、暗号化アルゴリズムＥ５は、ＤＥＳにより規定されたものである。

（４）復号部２１５

復号部２１５は、第２記憶領域２２２が有する暗号化ソフトウェア管理情報テーブル２３１ｃから暗号化ソフトウェア管理情報を読み出し、キー情報記憶部２１７からキー情報を読み出す。

【０１３９】

次に、復号部２１５は、読み出したキー情報を用いて、読み出した暗号化ソフトウェア管理情報に復号アルゴリズムＤ５を施して、ソフトウェア管理情報を生成し、生成したソフトウェア管理情報を判定部２１４へ出力する。

ここで、復号アルゴリズムＤ５は、ＤＥＳにより規定されたものであり、暗号化アルゴリズムＥ５に対応するものである。復号アルゴリズムＤ５は、暗号化アルゴリズムＥ５を用いて生成された暗号文を復号する。

【０１４０】

３．２　情報処理装置３００ｃの構成

情報処理装置３００ｃは、図１３に示すように、インストール処理部３１０、ソフトウェア格納部３２０、制御部３２１、表示部３２２、入力部３２３、ソフトウェア実行部３２４及び復号部３２５から構成されている。インストール処理部３１０は、さらに、認証部３１１、暗号化部３１２、復号部３１３、復号部３１４、暗号化部３１５、装置ＩＤ格納部３１６、装置固有鍵生成部３１７、ソフトＩＤ取得部３１８及び署名検証部３１９から構成されている。

【０１４１】

このように、情報処理装置３００ｃは、情報処理装置３００ｂと同様の構成を有しているので、詳細についての説明を省略する。

３．３　その他の例

変形例（２）では、キー情報記憶部２１７に記憶されているキー情報は固定値であるとしているが、これに限定されることなく、キー情報は、可変値であるとしてもよい。

【０１４２】

この場合、第２記憶領域２２２から判定部２１４へソフトウェア管理情報を出力する際に、復号部２１５は、暗号化ソフトウェア管理テーブル２３１ｃから全ての暗号化ソフトウェア管理情報を読み出し、キー情報記憶部２１７からキー情報を読み出し、次に復号部２１５は、読み出したキー情報を用いて読み出した全暗号化ソフトウェア管理情報に復号アルゴリズムＤ５を施してソフトウェア管理情報を生成する。次に、判定部２１４から第２記憶領域２２２へソフトウェア管理情報を出力する際に、判定部２１４は、キー情報を更新してキー情報記憶部２１７に格納し、暗号化部２１６は、更新されたキー情報を用いて、復号された全ソフトウェア管理情報に、暗号化アルゴリズムＥ５を施して暗号化ソフトウェア管理情報を生成し、第２記憶領域２２２の暗号化ソフトウェア管理テーブル２３１ｃに書き込むとしても良い。

【０１４３】

４．変形例（３）

変形例（１）に示すソフトウェア管理システム１０ｂの変形例としてのソフトウェア管理システム１０ｄ（図示していない）について説明する。

ソフトウェア管理システム１０ｄは、ソフトウェア書込装置１００ｄ（図示していない）、可搬型のメモリカード２００ｄ及び情報処理装置３００ｄから構成されている。ソフトウェア書込装置１００ｄ、メモリカード２００ｄ及び情報処理装置３００ｄは、それぞれソフトウェア書込装置１００ｂ、メモリカード２００ｂ及び情報処理装置３００ｂと同様の構成を有している。

【０１４４】

ここでは、メモリカード２００ｂとの相違点を中心として、メモリカード２００ｄについて説明する。

メモリカード２００ｄは、図１４に示すように、耐タンパモジュール部２１０及び情報記憶部２２０から構成されている。耐タンパモジュール部２１０は、認証部２１１、復号部２１２、暗号化部２１３、判定部２１４及び情報記憶部２１８から構成されている。メモリカード２００ｂが有する耐タンパモジュール部２１０とは、メモリカード２００ｄが有する耐タンパモジュール部２１０がさらに情報記憶部２１８を有している点において、相違している。

【０１４５】

（１）情報記憶部２１８

情報記憶部２１８は、図１５に一例として示す部分ソフトウェア管理テーブル２１９を有している。

部分ソフトウェア管理テーブル２１９は、複数個の部分ソフトウェア管理情報を記憶するための領域を備えている。各部分ソフトウェア管理情報は、ソフトＩＤ及び前半ソフト署名データから構成されている。

【０１４６】

ここで、ソフトＩＤについては、上述した通りであるので、説明を省略する。

前半ソフト署名データは、上述したソフト署名データを構成するビット列のうち、前半の部分のビット列から構成されている。具体的には、前半ソフト署名データは、１６０ビット長のビット列から構成されている。

（２）ソフトウェア管理情報テーブル２３１

ソフトウェア管理情報テーブル２３１は、図１５に示すように、一例として、ソフトウェア管理情報２４１ｄ、・・・を記憶するための領域を備えている。

【０１４７】

ソフトウェア管理情報２４１ｄは、ソフトＩＤ、ソフトキー、インストール回数情報、後半ソフト署名データ、及び複数の装置ＩＤを含んでいる。

ここで、ソフトＩＤ、ソフトキー、インストール回数情報及び複数の装置ＩＤについては、上述した通りであるので説明を省略する。

後半ソフト署名データは、上述したソフト署名データを構成するビット列のうち、後半の部分のビット列から構成されている。具体的には、後半ソフト署名データは、１６０ビット長のビット列から構成されている。

【０１４８】

（３）判定部２１４

判定部２１４は、認証部２１１から第１認証成功情報を受け取ると、さらに、ソフト署名データを受け取る。次に、判定部２１４は、受け取ったソフト署名データを、２個のビット列に分割して、前半ソフト署名データ及び後半ソフト署名データを生成する。分割して生成された前半のビット列が前半ソフト署名データであり、後半のビット列が後半ソフト署名データである。前半ソフト署名データ及び後半ソフト署名データは、それぞれ、１６０ビット長である。

【０１４９】

次に、判定部２１４は、生成した前半ソフト署名データ及び受け取ったソフトＩＤから構成される部分ソフトウェア管理情報を生成し、生成した部分ソフトウェア管理情報を情報記憶部２１８が有する部分ソフトウェア管理テーブル２１９内に書き込む。また、判定部２１４は、生成した後半ソフト署名データを含むソフトウェア管理情報をソフトウェア管理情報テーブル２３１内に追加して書き込む。

【０１５０】

また、判定部２１４は、部分ソフトウェア管理テーブル２１９から、ソフトＩＤを含む部分ソフトウェア管理情報を読み出し、ソフトウェア管理テーブル２３１から、ソフトＩＤを含むソフトウェアか管理情報を読み出す。次に、判定部２１４は、読み出した部分ソフトウェア管理情報から前半ソフト署名データを抽出し、読み出したソフトウェア管理情報から後半ソフト署名データを抽出し、抽出

した前半ソフト署名データ及び抽出した後半ソフト署名データを結合してソフト署名データを生成する。

【０１５１】

以上説明したように、耐タンパモジュール部２１０は、さらに、情報記憶部２１８を備え、情報記憶部２１８は、ソフトウェア管理テーブルの一部を格納する。

具体的には、一例として、情報記憶部２１８は、ソフト署名データの少なくとも一部を格納する。第２記憶領域２２２が有するソフトウェア管理テーブル２３１は、ソフト署名データの残りの部分を格納する。判定部２１４は、情報記憶部２１８に含まれるソフト署名データの少なくとも一部と、第２記憶領域２２２から読み出したソフト管理情報に含まれるソフト署名データの残りの部分より、ソフト署名データ全体を復元して使用する。

【０１５２】

なお、ここでは、情報記憶部２１８にソフト署名データの前半部分を格納する構成について説明したが、この構成に限定されるものではない。

５．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【０１５３】

（１）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ―ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０１５４】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０１５５】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（２）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０１５６】

【発明の効果】

以上説明したように、本発明は、ソフトウェアを記録している記録媒体と、前記ソフトウェアを内部に記録し、前記ソフトウェアに従って動作する情報処理装置とから構成される情報処理システムであって、前記記録媒体は、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備え、前記情報処理装置は、前記ソフトウェアを記憶するための領域を備える記憶手段と、前記記録媒体から前記許可指示を取得する取得手段と、取得した前記許可指示に応じて、前記記録媒体か

ら前記ソフトウェアを取得して前記記憶手段に書き込み、又は前記記憶手段に記憶されている前記ソフトウェアを非活性化する制御手段とを備える。また、ソフトウェアを記録している記録媒体であって、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備える。また、ソフトウェアを記録している記録媒体から、前記ソフトウェアを取得して内部に記録し、前記ソフトウェアに従って動作する情報処理装置であって、前記記録媒体は、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備え、前記情報処理装置は、前記ソフトウェアを記憶するための領域を備える記憶手段と、前記記録媒体から前記許可指示を取得する取得手段と、取得した前記許可指示に応じて、前記記録媒体から前記ソフトウェアを取得して前記記憶手段に書き込み、又は前記記憶手段に記憶されている前記ソフトウェアを非活性化する制御手段とを備える。

【０１５７】

これらの構成によると、外部から直接アクセスできないセキュア記憶手段にライセンス情報が記憶されているので、ライセンス情報の改竄が容易ではない。また、記録媒体から相手装置へライセンス情報が伝送されないので、記録媒体から

相手装置への通信路上においてライセンス情報が漏洩して改竄されることはない。さらに、ソフトウェアの使用条件に係るライセンス情報がセキュア記憶手段に記憶されているので、ライセンス情報とソフトウェアとの対応関係が不当に改竄されることはない。

【０１５８】

ここで、前記通常記憶手段は、ソフトキーを用いて暗号化された暗号化ソフトウエアを記憶しており、前記セキュア記憶手段は、前記ソフトキーを含む前記ライセンス情報を記憶しており、前記耐タンパモジュール手段は、インストール可と判断する場合に、前記セキュア記憶領域に記憶されているライセンス情報からソフトキーを抽出し、抽出したソフトキーをセキュアに出力する。

【０１５９】

この構成によると、暗号化ソフトウェアを暗号化するために用いられるソフトキーを、耐タンパモジュール手段がセキュアに出力するので、ソフトキーが不当に改竄されることがない。

ここで、前記セキュア記憶手段は、前記ソフトウェアの署名データを含む前記使用条件に係る前記ライセンス情報を記憶しており、前記耐タンパモジュール手段は、インストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報から前記署名データを抽出し、抽出した前記署名データを出力する。

【０１６０】

この構成によると、耐タンパモジュール手段がソフトウェアの署名データを出力するので、署名データが改竄されることはない。

ここで、前記セキュア記憶手段は、前記使用条件が所定のキー情報を用いて暗号化されて生成された前記ライセンス情報を記憶しており、前記耐タンパモジュール手段は、前記キー情報を記憶しており、前記キー情報を用いて、前記ライセンス情報を復号して前記使用条件を生成し、生成した使用条件に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する。

【０１６１】

この構成によると、前記セキュア記憶手段は、前記使用条件が所定のキー情報を用いて暗号化されて生成された前記ライセンス情報を記憶しており、前記耐タンパモジュール手段は、記憶している前記キー情報を用いて、前記ライセンス情報を復号して前記使用条件を生成するので、正当なキー情報を記憶している前記耐タンパモジュール手段のみが前記ライセンス情報を使用することができる。

【０１６２】

ここで、前記セキュア記憶手段は、前記ライセンス情報の一部分を記憶しており、前記耐タンパモジュール手段は、さらに、前記ソフトウェアの他の部分を記憶しており、インストール又はアンインストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報の前記一部分を抽出し、抽出した前記一部分と記憶している前記他の部分とからライセンス情報を生成する。

【０１６３】

この構成によると、前記セキュア記憶手段は、ライセンス情報の一部分を記憶しており、前記耐タンパモジュール手段は、前記ライセンス情報の他の部分を記憶しており、これらから全体のライセンス情報を生成するので、ライセンス情報が改竄される可能性をさらに低減することができる。

ここで、前記セキュア記憶手段が記憶しているライセンス情報は、前記ソフトウェアの使用許可回数であり、前記耐タンパモジュール手段は、前記使用許可回数が０より大きいか否かを判断し、０より大きいと判断する場合に、前記ソフトウェアの使用が許可されたとみなして、前記許可指示、前記ソフトキー、もしくは前記署名データのうち、少なくとも一つを出力し、さらに、前記使用許可回数から１減じて前記セキュア記憶手段に書き込む。

【０１６４】

この構成によると、前記ライセンス情報は、前記ソフトウェアの使用許可回数であり、インストールの際に、前記耐タンパモジュール手段は、前記使用許可回数が０より大きいと判断する場合に、前記使用許可回数から１を減じて前記セキュア記憶手段に書き込むので、前記ソフトウェアの使用回数を確実に管理することができる。

【０１６５】

ここで、前記セキュア記憶手段が記憶しているライセンス情報は、前記ソフトウェアの使用許可回数であり、前記耐タンパモジュール手段は、前記ソフトウエアのアンインストールが許可された場合に、前記許可指示を出力し、さらに、前記使用許可回数を１加算して前記セキュア記憶手段に書き込む。

この構成によると、前記ライセンス情報は、前記ソフトウェアの使用許可回数であり、アンインストールの際に、前記使用許可回数に１を加算して前記セキュア記憶手段に書き込むので、前記ソフトウェアの使用回数を確実に管理することができる。

【０１６６】

また、本発明は、ソフトウェアを記録している記録媒体であって、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断し、許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出し、読み出した前記署名データを出力する耐タンパモジュール手段とを備える。

【０１６７】

この構成によると、外部から直接アクセスできないセキュア記憶手段にライセンス情報が記憶されているので、ライセンス情報の改竄が容易ではない。また、記録媒体から相手装置へライセンス情報が伝送されないので、記録媒体から相手装置への通信路上においてライセンス情報が漏洩して改竄されることはない。さらに、ライセンス情報とソフトウェアの署名データとがセキュア記憶手段に記憶されているので、ライセンス情報とソフトウェアとの対応関係が不当に改竄されることはない。

【０１６８】

また、ソフトウェアを記録している記録媒体から前記ソフトウェアを読み出して内部に記憶する情報処理装置であって、前記記録媒体は、ソフトウェアを記憶

している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断し、許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出し、読み出した前記署名データを出力する耐タンパモジュール手段とを備え、前記情報処理装置は、前記記録媒体から前記署名データ及び前記ソフトウェアを取得する取得手段と、取得した前記署名データを用いて、取得した前記ソフトウェアの検証を行い、検証が成功した場合に、取得した前記ソフトウェアを内部に記憶する記憶手段とを備える。

【０１６９】

この構成によると、前記記録媒体から取得した前記署名データを用いて、取得した前記ソフトウェアの検証を行い、検証が成功した場合に、取得した前記ソフトウェアを内部に記憶するので、正当なソフトウェアのみを取得して内部に記憶することができる。

【図面の簡単な説明】

【図１】

ソフトウェア管理システム１０の構成を示す。

【図２】

ソフトウェア書込装置１００及びメモリカード２００の構成を示すブロック図である。

【図３】

メモリカード２００及び情報処理装置３００の構成を示すブロック図である。

【図４】

ソフトウェア管理情報テーブル２３１のデータ構造の一例を示す。

【図５】

ソフトウェア管理システム１０の動作を示すフローチャートである。特に、メモリカード２００から情報処理装置３００へソフトウェアがインストールされる場合、又はアンインストールされる場合の動作を示している。図６へ続く。

【図６】

ソフトウェア管理システム１０の動作を示すフローチャートである。特に、メモリカード２００から情報処理装置３００へソフトウェアがインストールされる場合、又はアンインストールされる場合の動作を示している。図７へ続く。

【図７】

ソフトウェア管理システム１０の動作を示すフローチャートである。特に、メモリカード２００から情報処理装置３００へソフトウェアがインストールされる場合、又はアンインストールされる場合の動作を示している。図８へ続く。

【図８】

ソフトウェア管理システム１０の動作を示すフローチャートである。特に、メモリカード２００から情報処理装置３００へソフトウェアがインストールされる場合、又はアンインストールされる場合の動作を示している。図７から続く。

【図９】

判定部２１４における詳細の動作を示すフローチャートである。

【図１０】

変形例としてのソフトウェア管理システム１０ｂを構成するソフトウェア書込装置１００ｂ及びメモリカード２００ｂの構成を示すブロック図である。

【図１１】

ソフトウェア管理情報のデータ構造の一例を示す。

【図１２】

ソフトウェア管理システム１０ｂを構成するメモリカード２００ｂ及び情報処理装置３００ｂの構成を示すブロック図である。

【図１３】

別の変形例としてのソフトウェア管理システム１０ｃを構成するメモリカード２００ｃ及び情報処理装置３００ｃの構成を示すブロック図である。

【図１４】

別の変形例としてのソフトウェア管理システム１０ｄを構成するメモリカード２００ｄ及び情報処理装置３００ｄの構成を示すブロック図である。

【図１５】

部分ソフトウェア管理テーブル２１９及びソフトウェア管理情報テーブル２３１の一例としてのデータ構造を示す。

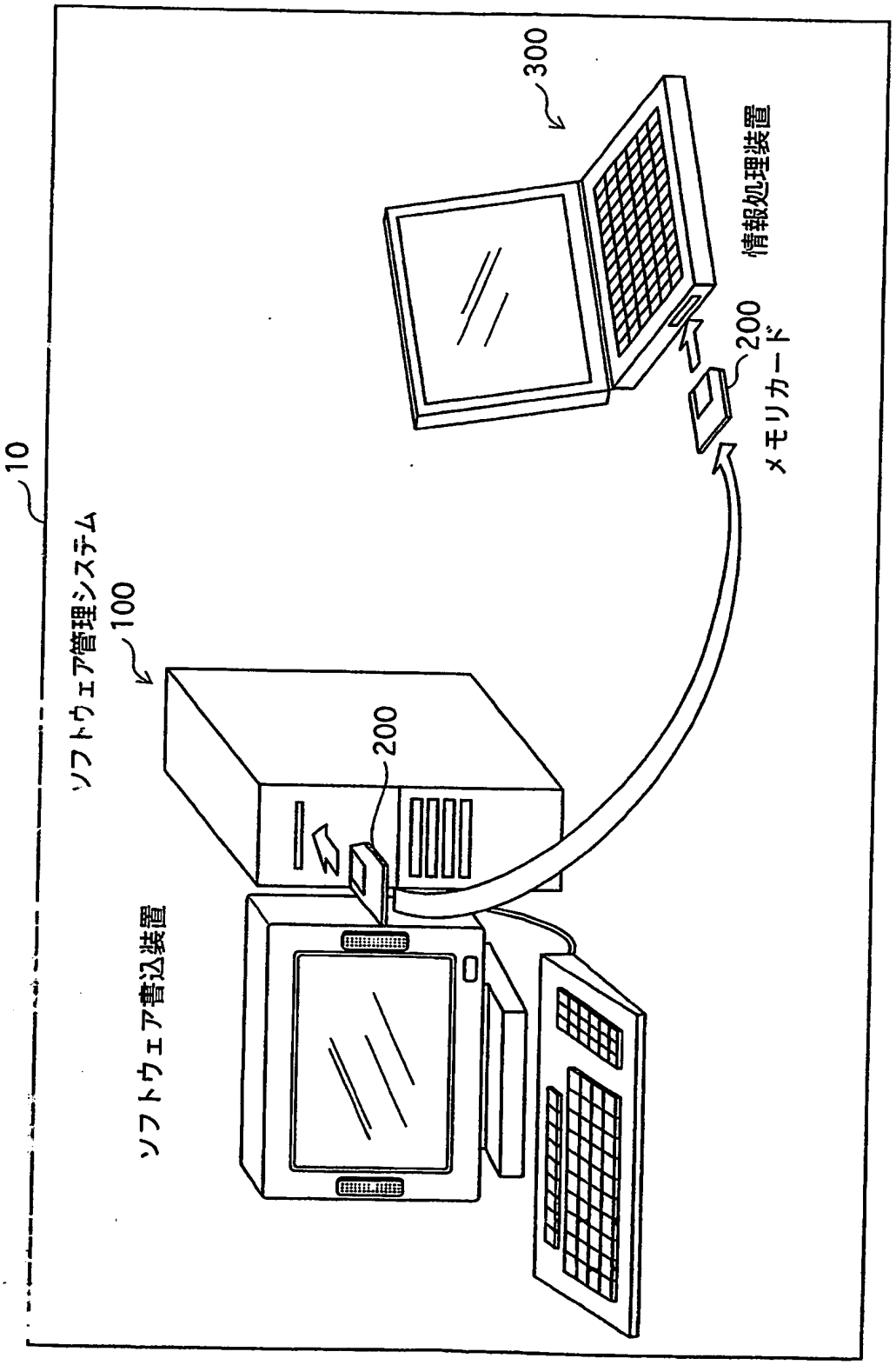
【符号の説明】

１０	ソフトウェア管理システム
１００	ソフトウェア書込装置
１１１	認証部
１１２	暗号化部
１１３	情報記憶部
１１４	制御部
１１５	入力部
１１６	表示部
１１７	署名生成部
１１８	入出力部
２００	メモリカード
２１０	耐タンパモジュール部
２１１	認証部
２１２	復号部
２１３	暗号化部
２１４	判定部
２１５	復号部
２１６	暗号化部
２１７	キー情報記憶部
２２０	情報記憶部
３００	情報処理装置
３１０	インストール処理部
３１１	認証部
３１２	暗号化部
３１３	復号部
３１４	復号部

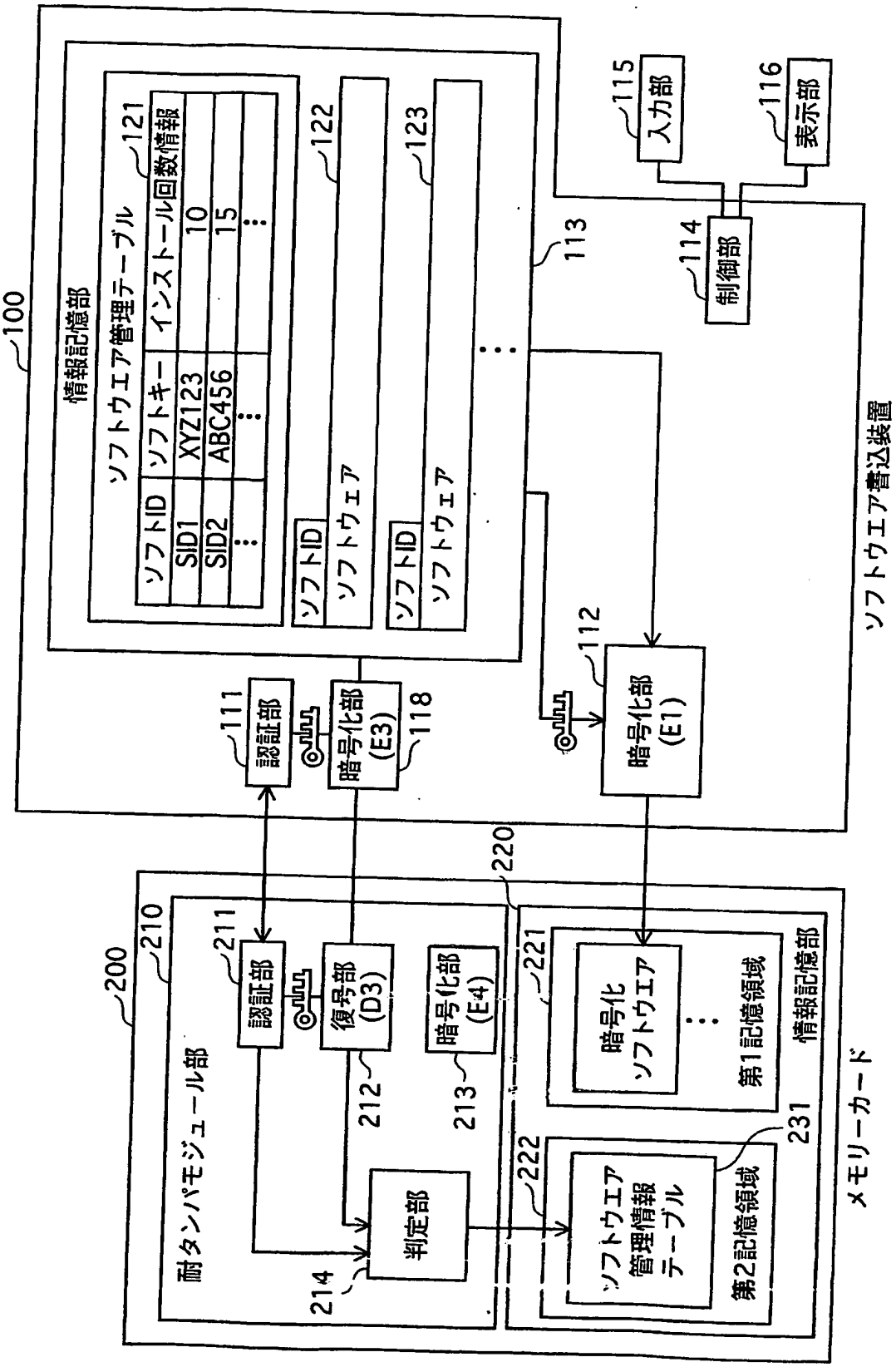
３１５　暗号化部
３１６　装置ＩＤ格納部
３１７　装置固有鍵生成部
３１８　ソフトＩＤ取得部
３１９　署名検証部
３２０　ソフトウェア格納部
３２１　制御部
３２２　表示部
３２３　入力部
３２４　ソフトウェア実行部
３２５　復号部

【書類名】　図面

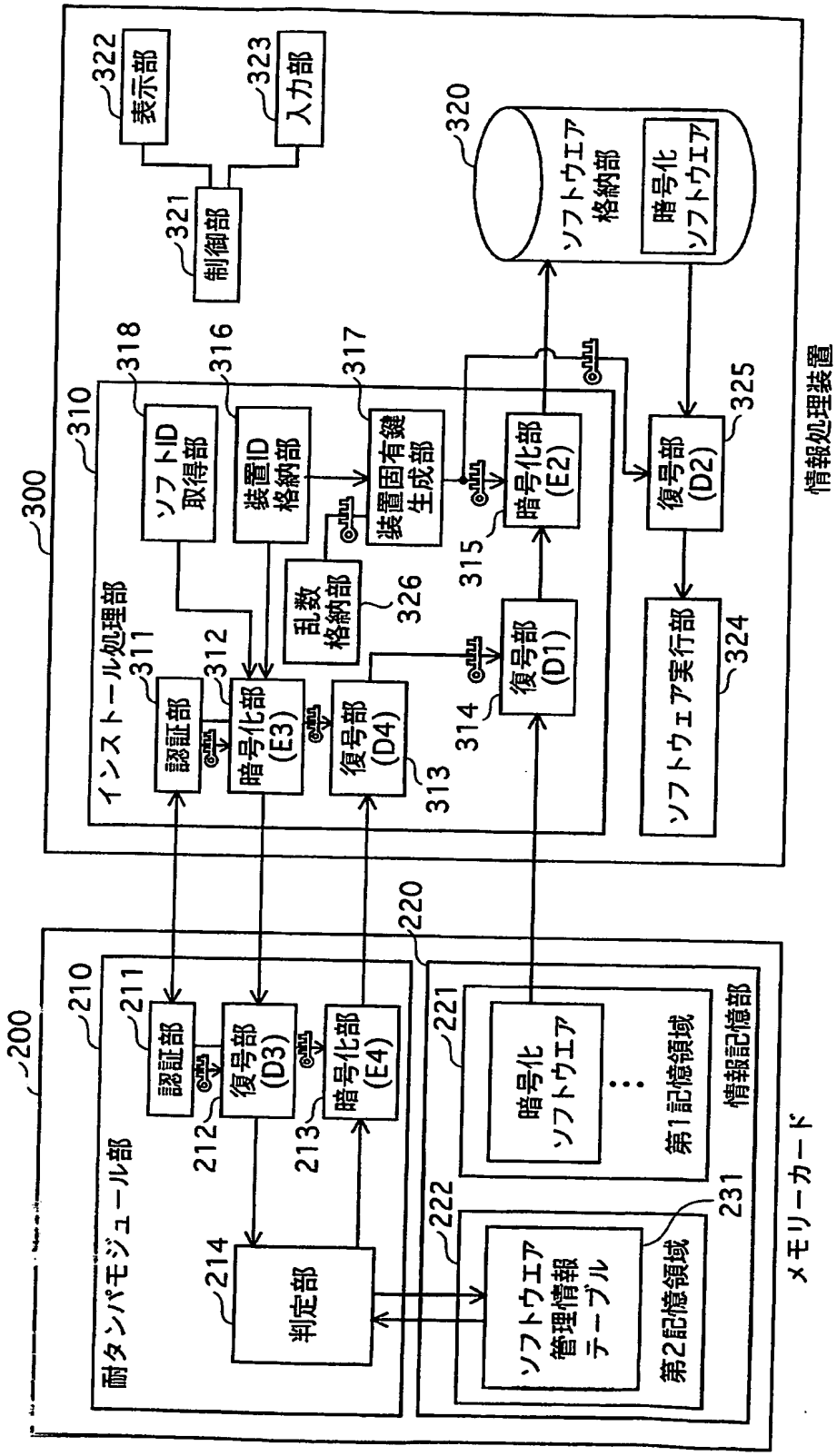
【図１】



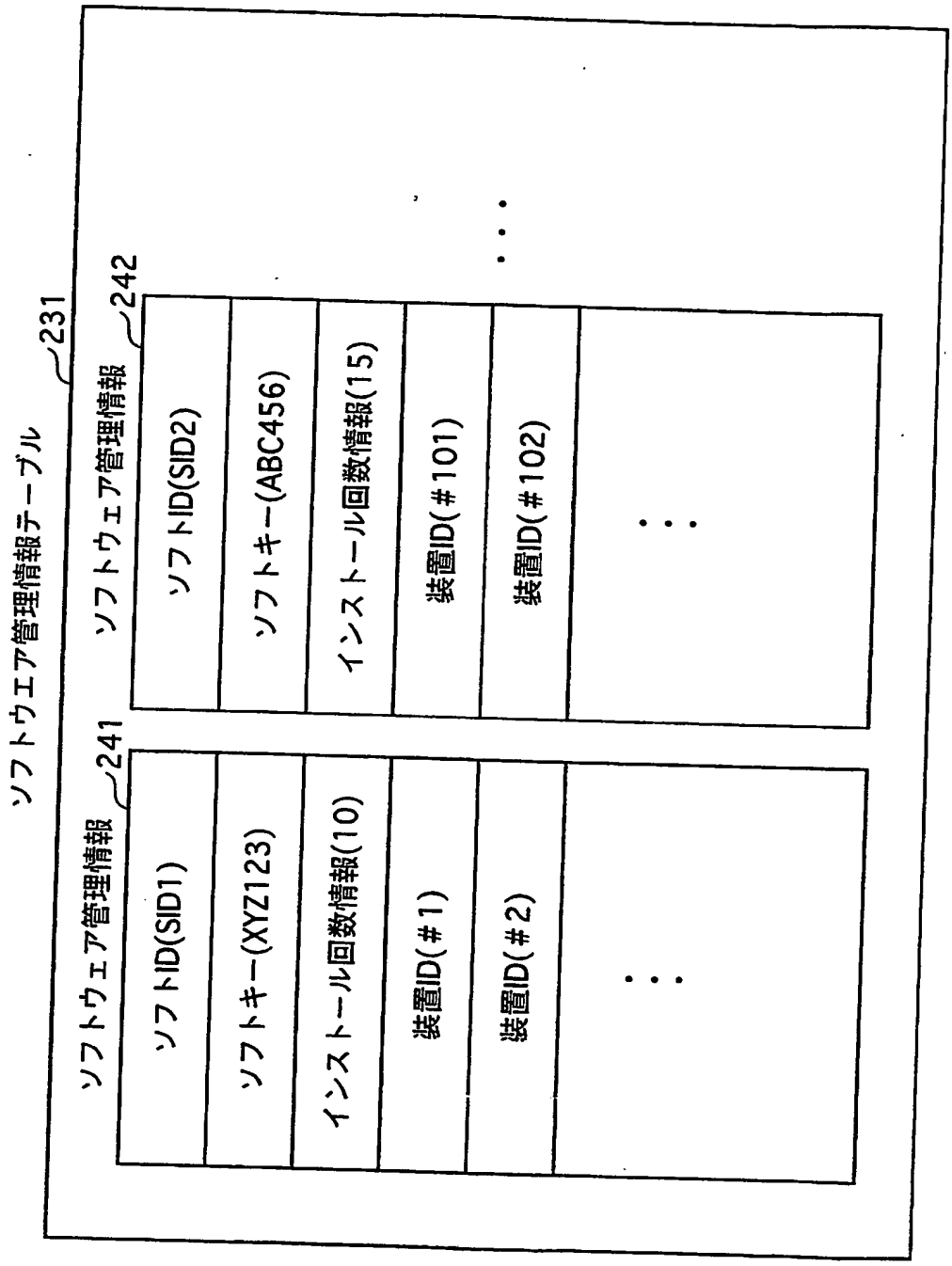
【図２】


100
情報記憶部
ソフトウエア管理テーブル
121
ソフトID
ソフトキー
インストール回数情報
SID1
XYZ123
10
SID2
ABC456
15
122
ソフトID
ソフトウェア
123
ソフトID
ソフトウェア
113
115
入力部
116
表示部
114
制御部
111
認証部
暗号化部
(E3)
118
112
暗号化部
(E1)
ソフトウエア書込装置
220
200
210
211
認証部
復号部
(D3)
暗号化部
(E4)
221
暗号化
ソフトウエア
第1記憶領域
情報記憶部
耐タンパモジュール部
212
213
231
222
判定部
ソフトウエア
管理情報
テーブル
第2記憶領域
214
メモリーカード

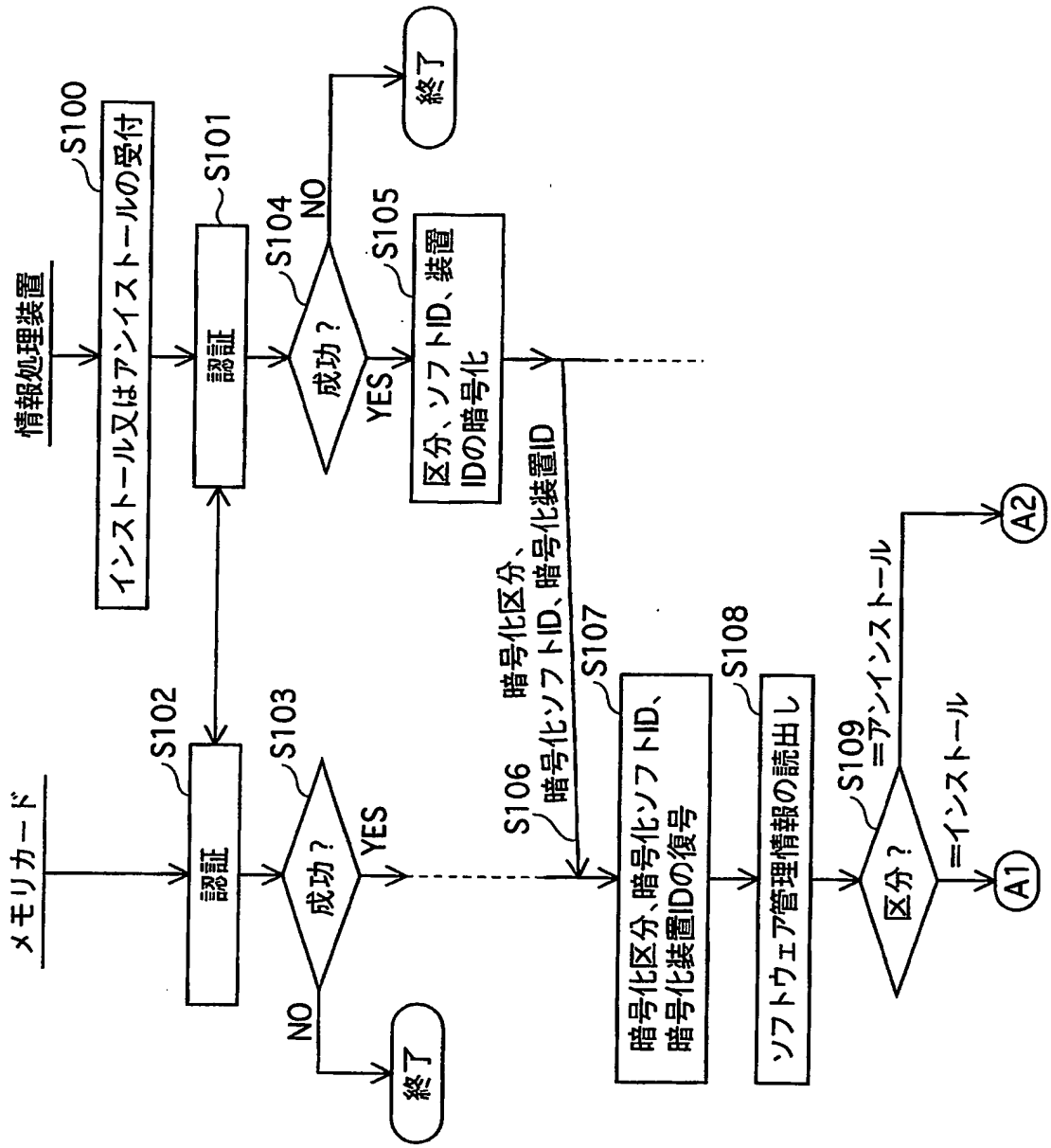
【図３】


情報処理装置
300
インストール処理部
310
311
認証部
312
暗号化部 (E3)
313
復号部 (D4)
314
復号部 (D1)
315
暗号化部 (E2)
316
装置ID 格納部
317
装置固有鍵 生成部
318
ソフトID 取得部
320
ソフトウエア 格納部
暗号化 ソフトウエア
321
制御部
322
表示部
323
入力部
324
ソフトウェア実行部
325
復号部 (D2)
326
乱数 格納部
メモリーカード
200
耐タンパモジュール部
210
211
認証部
212
復号部 (D3)
213
暗号化部 (E4)
214
判定部
220
情報記憶部
221
暗号化 ソフトウエア
第1記憶領域
222
ソフトウエア 管理情報 テーブル
231
第2記憶領域

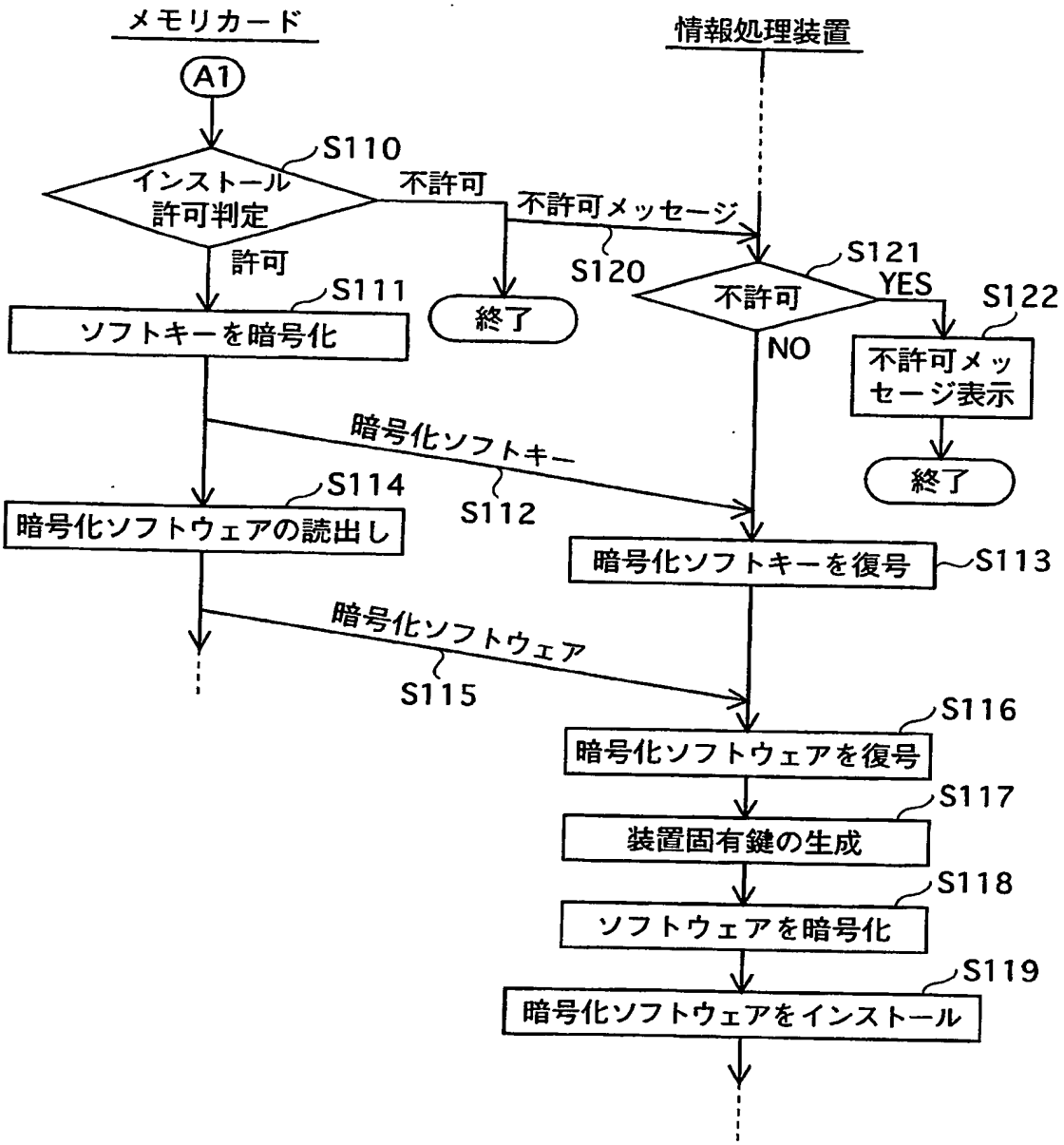
【図４】


ソフトウエア管理情報テーブル
231
ソフトウェア管理情報
241
ソフトID(SID1)
ソフトキー(XYZ123)
インストール回数情報(10)
装置ID(＃1)
装置ID(＃2)
ソフトウェア管理情報
242
ソフトID(SID2)
ソフトキー(ABC456)
インストール回数情報(15)
装置ID(＃101)
装置ID(＃102)

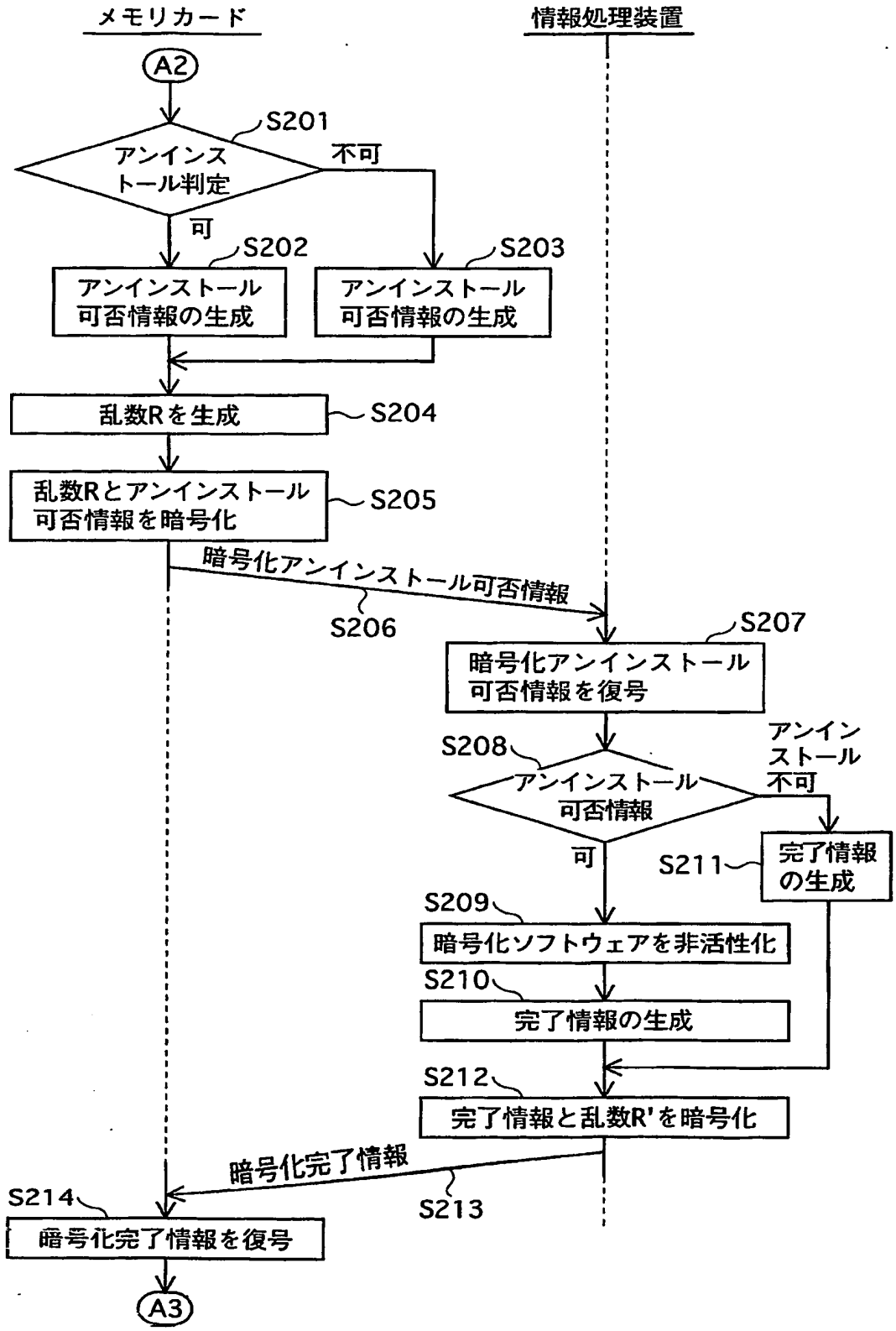
【図５】


情報処理装置
メモリカード
S100
インストール又はアンインストールの受付
S101
認証
S102
認証
S103
成功？
YES
NO
終了
S104
成功？
NO
YES
終了
S105
区分、ソフトID、装置IDの暗号化
S106
暗号化区分、暗号化ソフトID、暗号化装置ID
S107
暗号化区分、暗号化ソフトID、暗号化装置IDの復号
S108
ソフトウェア管理情報の読出し
S109
区分？
=アンインストール
=インストール
A1
A2

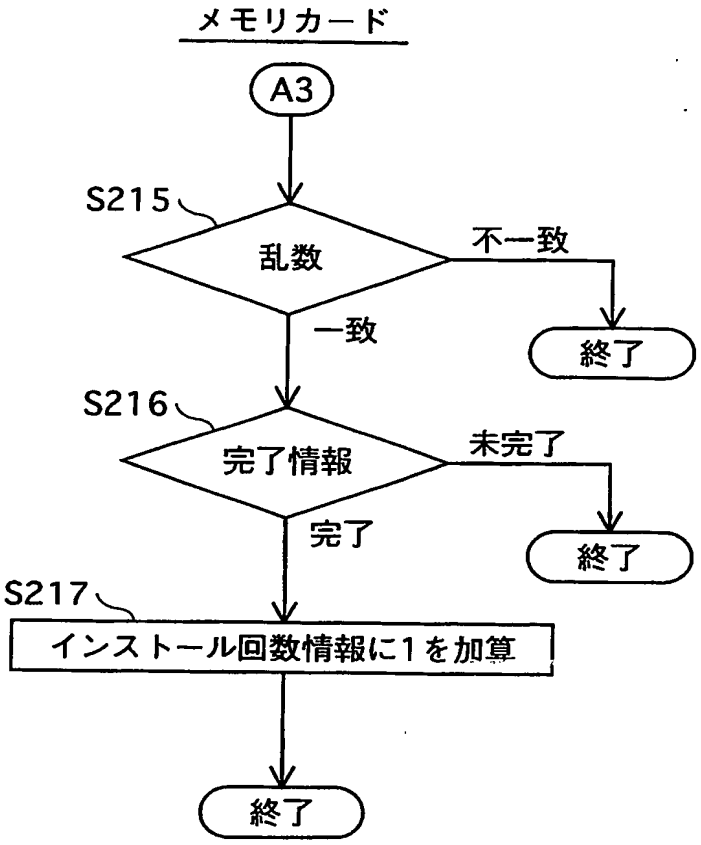
【図６】


メモリカード
情報処理装置
A1
S110
インストール
許可判定
不許可
許可
不許可メッセージ
S120
終了
S121
不許可
YES
NO
S122
不許可メッセージ表示
終了
S111
ソフトキーを暗号化
暗号化ソフトキー
S112
S114
暗号化ソフトウェアの読出し
暗号化ソフトキーを復号
S113
暗号化ソフトウェア
S115
S116
暗号化ソフトウェアを復号
S117
装置固有鍵の生成
S118
ソフトウェアを暗号化
S119
暗号化ソフトウェアをインストール

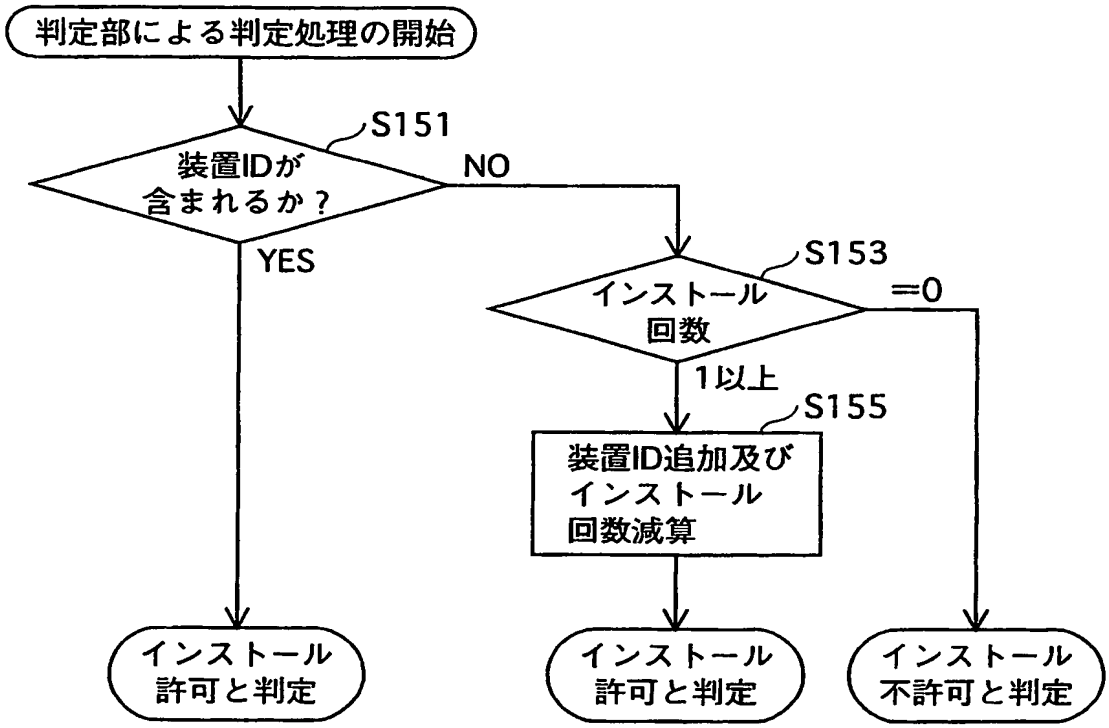
【図７】


メモリカード
情報処理装置
A2
S201
アンインストール判定
不可
可
S202
アンインストール可否情報の生成
S203
アンインストール可否情報の生成
乱数Rを生成
S204
乱数Rとアンインストール可否情報を暗号化
S205
暗号化アンインストール可否情報
S206
S207
暗号化アンインストール可否情報を復号
S208
アンインストール可否情報
アンインストール不可
可
S211
完了情報の生成
S209
暗号化ソフトウェアを非活性化
S210
完了情報の生成
S212
完了情報と乱数R'を暗号化
暗号化完了情報
S213
S214
暗号化完了情報を復号
A3

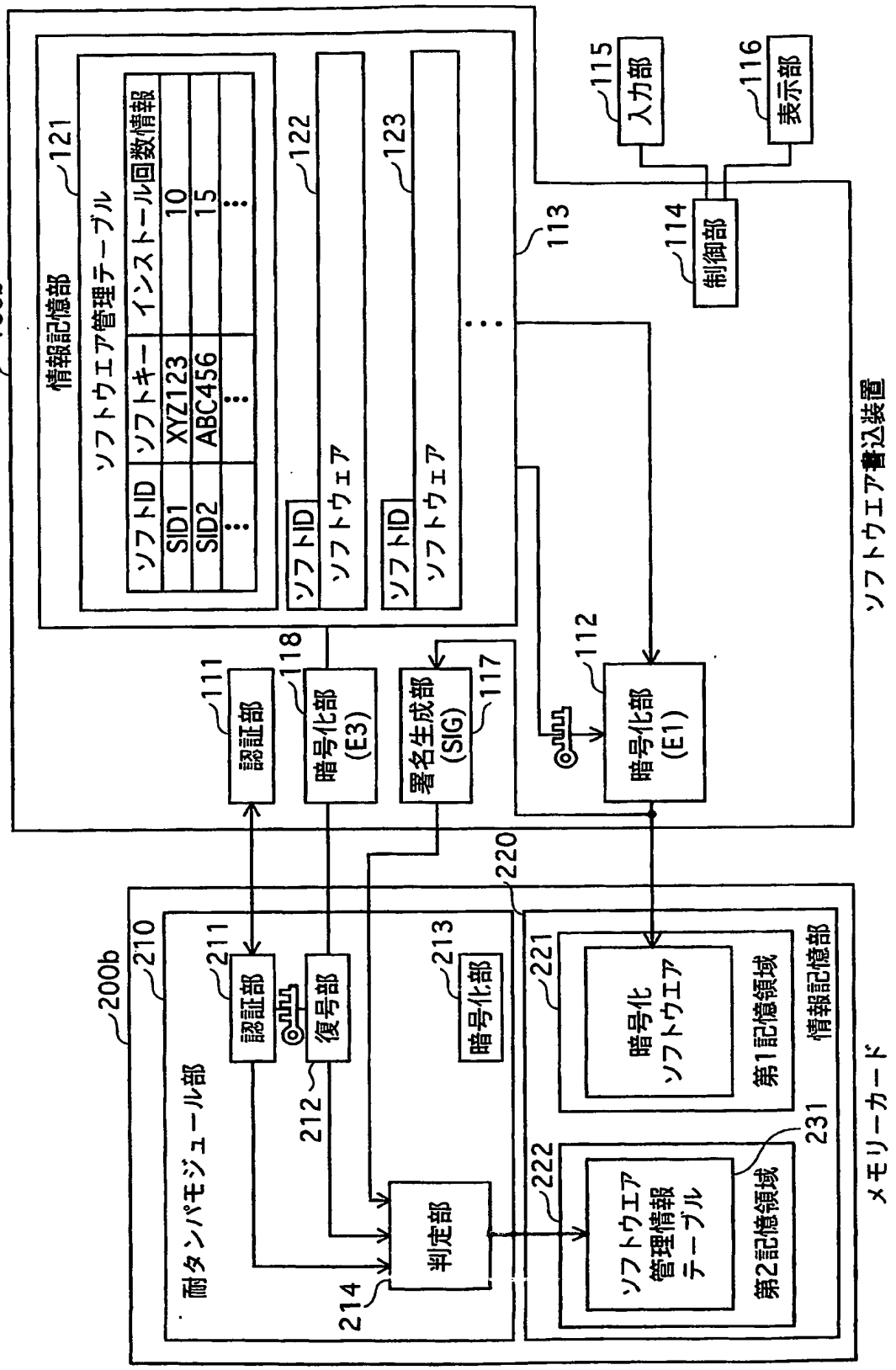
【図８】


メモリカード
A3
S215
乱数
不一致
一致
終了
S216
完了情報
未完了
完了
終了
S217
インストール回数情報に1を加算
終了

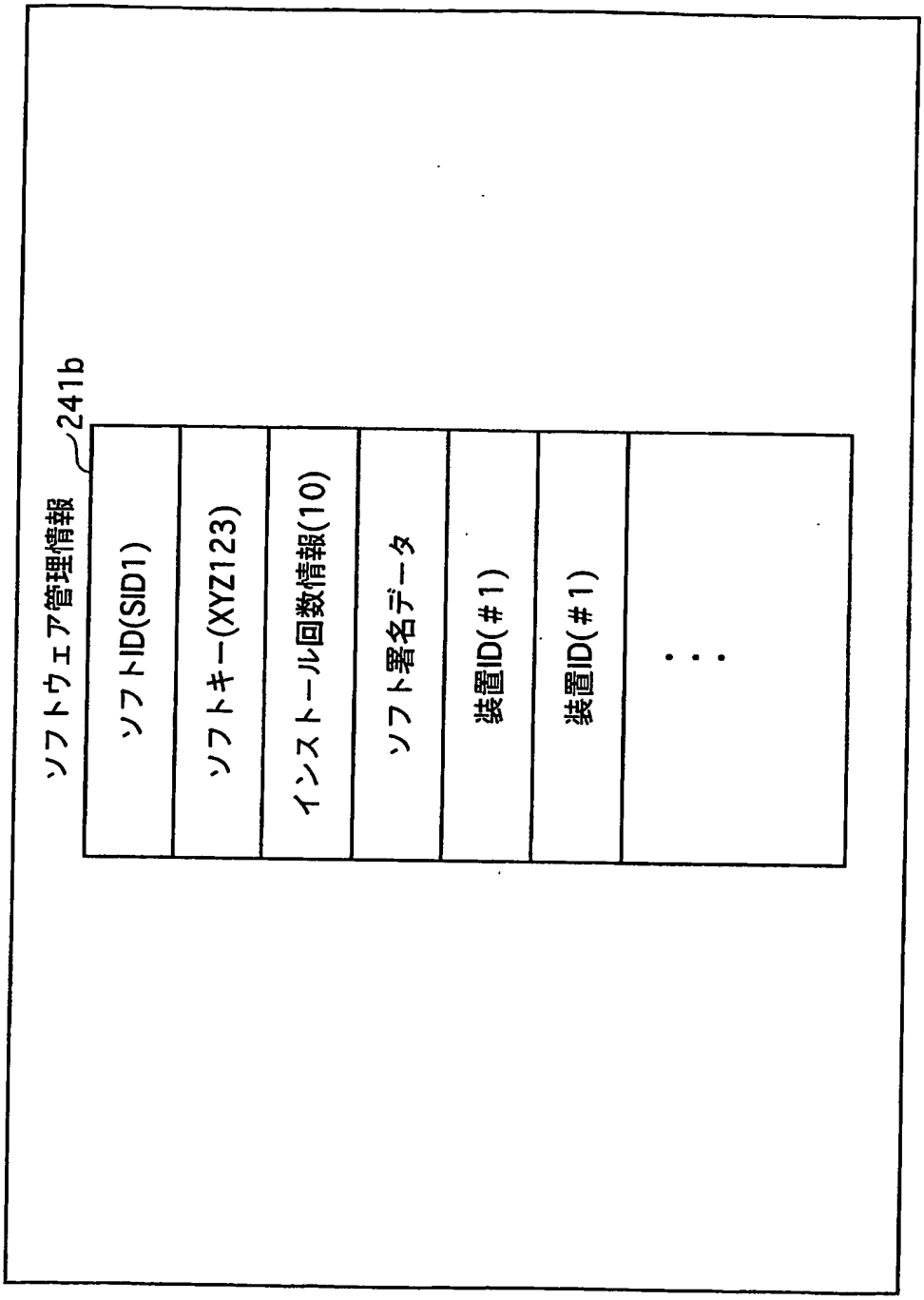
【図９】


判定部による判定処理の開始
S151
装置IDが
含まれるか？
NO
YES
S153
インストール
回数
=0
1以上
S155
装置ID追加及び
インストール
回数減算
インストール
許可と判定
インストール
許可と判定
インストール
不許可と判定

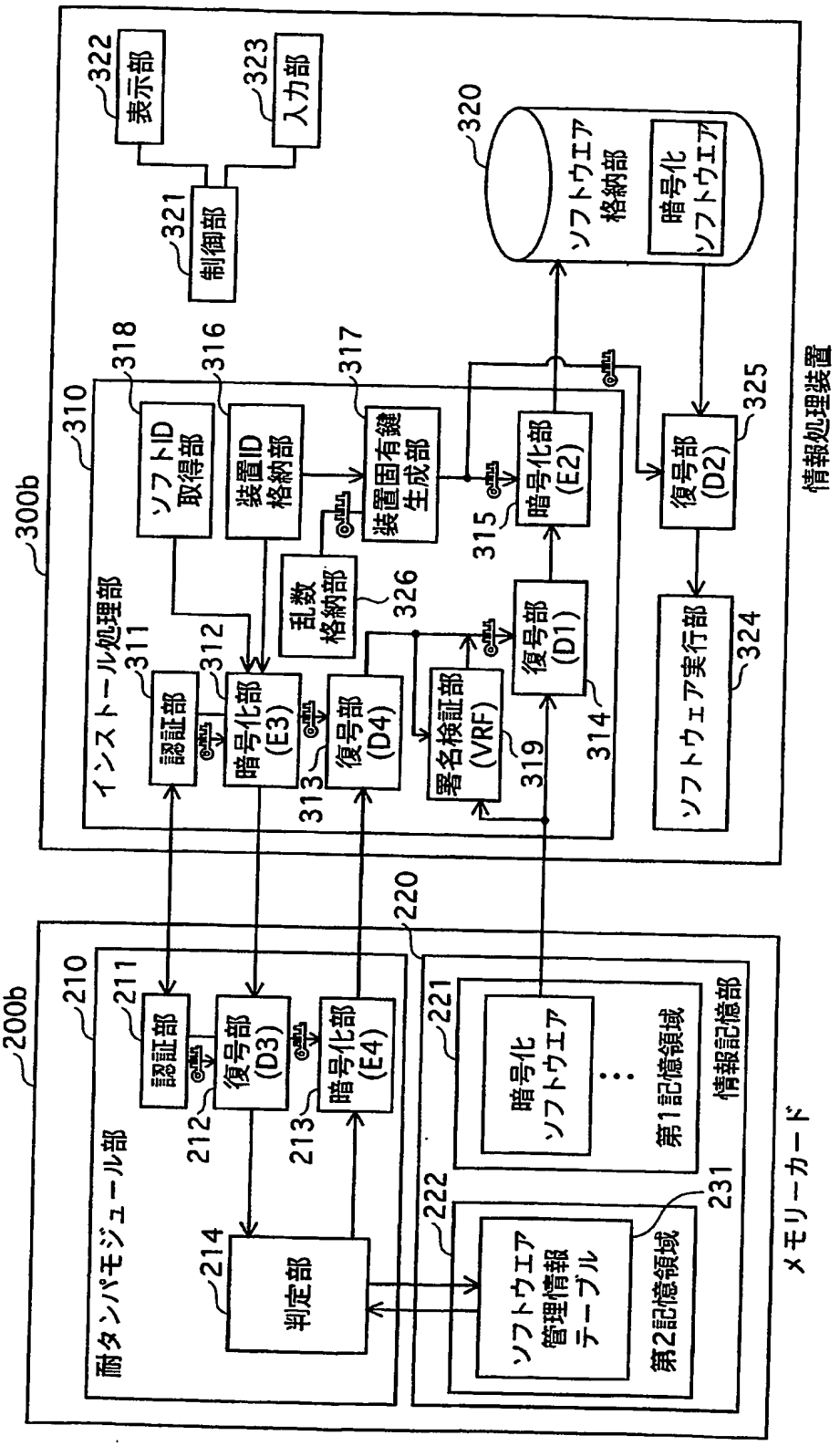
【図１０】


100b
情報記憶部
121
ソフトウエア管理テーブル
ソフトID
ソフトキー
インストール回数情報
SID1
XYZ123
10
SID2
ABC456
15
122
ソフトID
ソフトウェア
123
ソフトID
ソフトウェア
113
114
制御部
115
入力部
116
表示部
ソフトウエア書込装置
111
認証部
118
暗号化部
(E3)
署名生成部
(SIG)
117
112
暗号化部
(E1)
220
200b
210
耐タンパモジュール部
211
認証部
212
復号部
213
暗号化部
214
判定部
221
暗号化
ソフトウエア
第1記憶領域
情報記憶部
222
ソフトウエア
管理情報
テーブル
231
第2記憶領域
メモリーカード

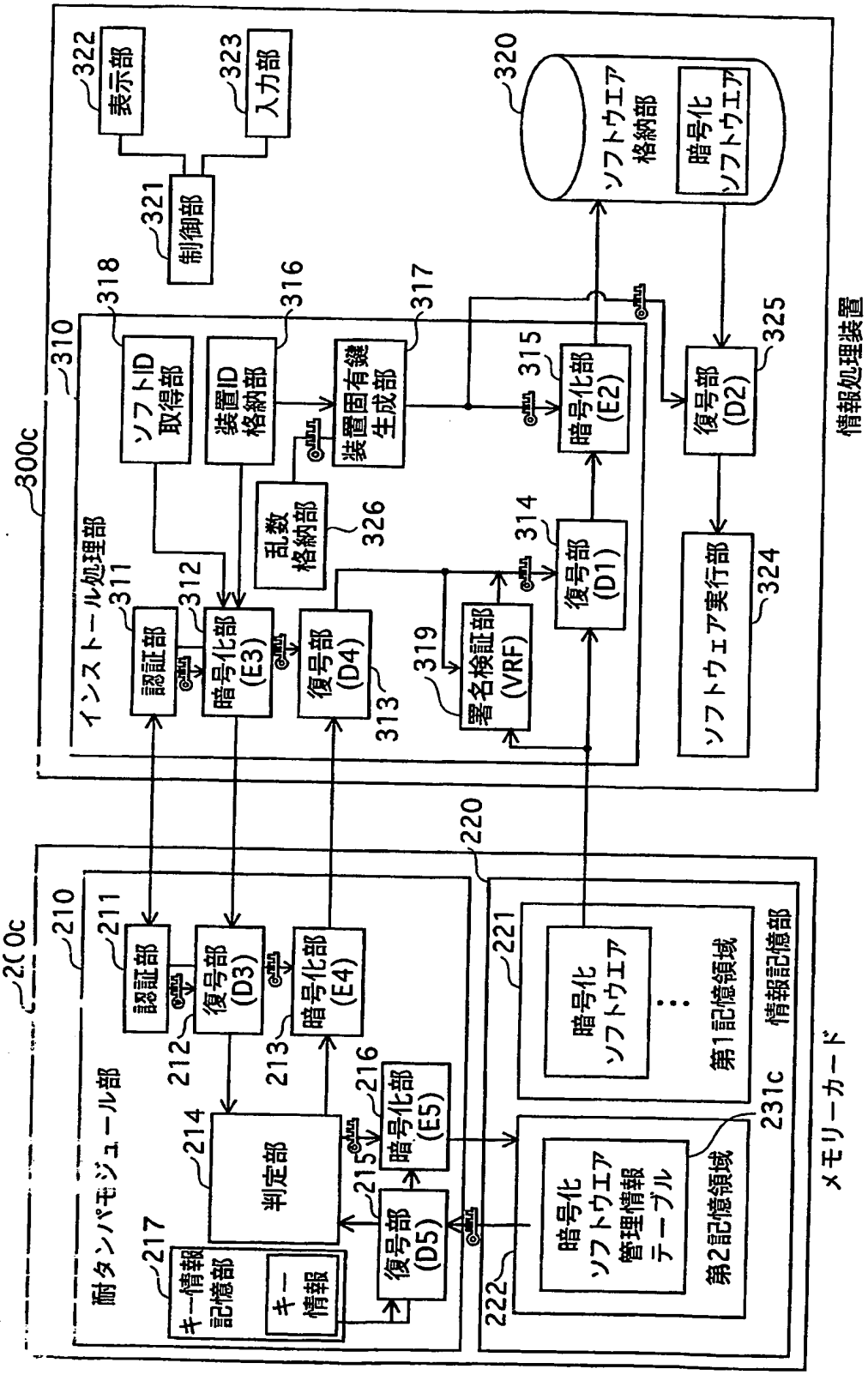
【図１１】


ソフトウェア管理情報
241b
ソフトID(SID1)
ソフトキー(XYZ123)
インストール回数情報(10)
ソフト署名データ
装置ID(＃1)
装置ID(＃1)
・・・

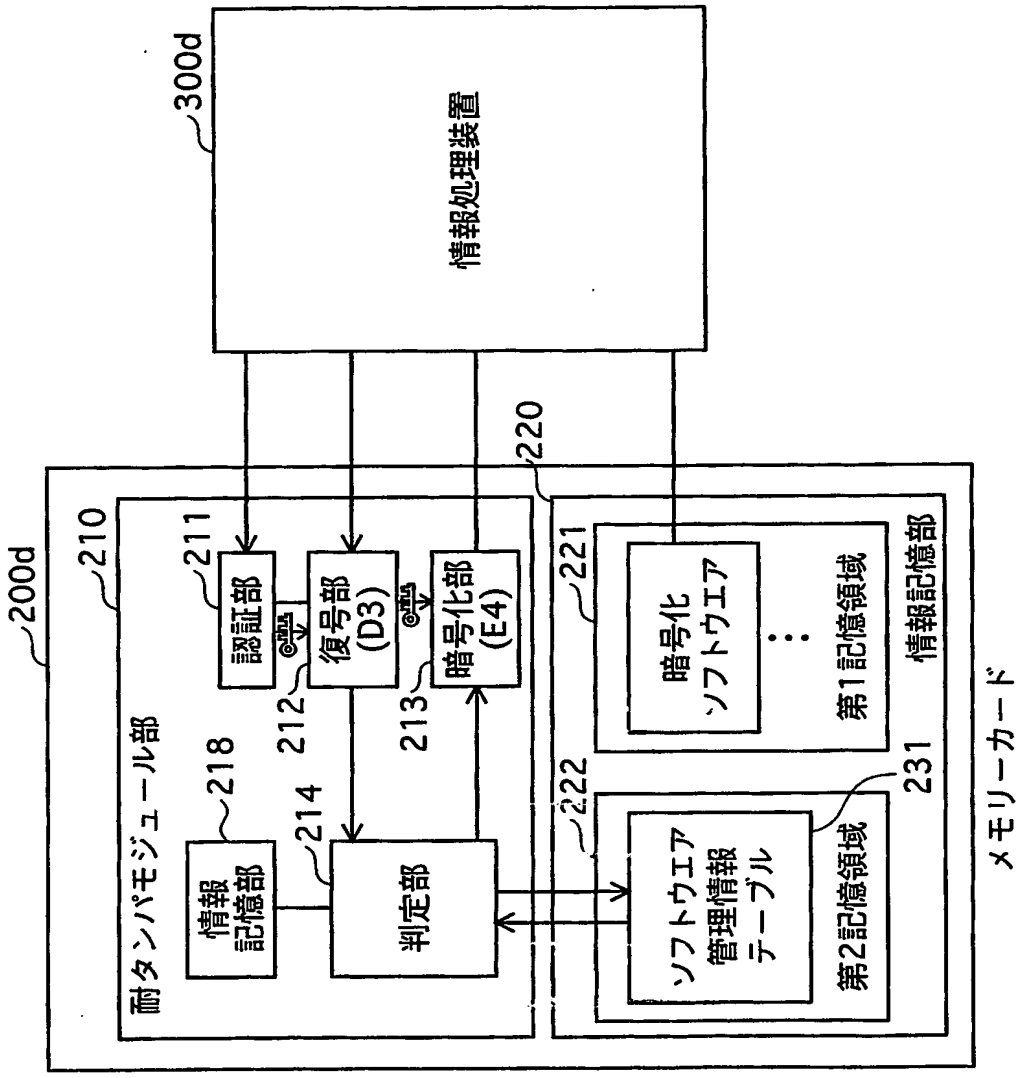
【図１２】


情報処理装置
300b
インストール処理部
310
ソフトID取得部
318
装置ID格納部
316
装置固有鍵生成部
317
乱数格納部
326
認証部
311
暗号化部(E3)
312
復号部(D4)
313
署名検証部(VRF)
319
復号部(D1)
314
暗号化部(E2)
315
ソフトウェア実行部
324
復号部(D2)
325
ソフトウエア格納部
320
暗号化ソフトウエア
制御部
321
表示部
322
入力部
323
メモリーカード
200b
耐タンパモジュール部
210
認証部
211
復号部(D3)
212
暗号化部(E4)
213
判定部
214
220
情報記憶部
221
暗号化ソフトウエア
第1記憶領域
222
ソフトウエア管理情報テーブル
第2記憶領域
231

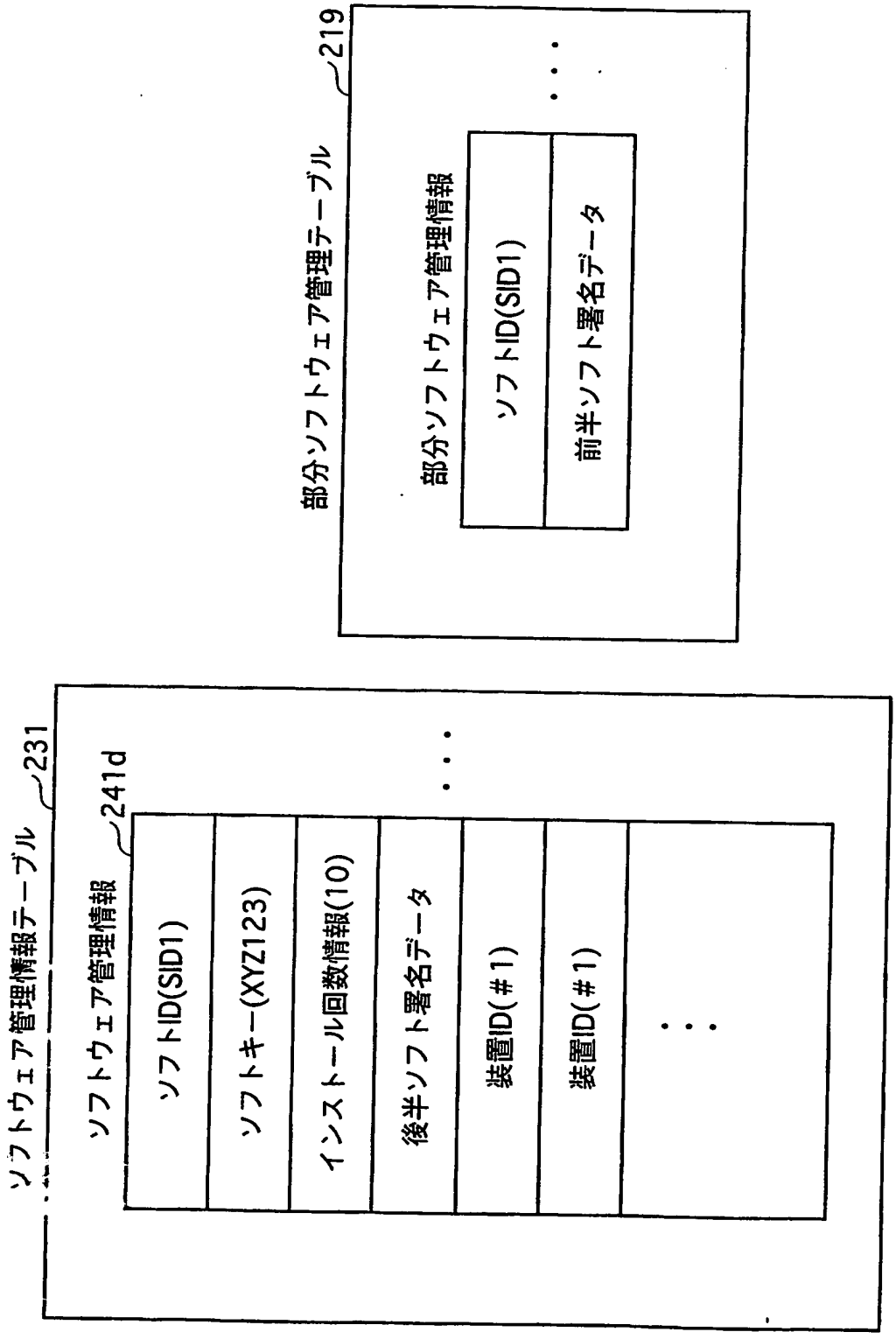
【図１３】


情報処理装置
300c
インストール処理部
310
311
認証部
312
暗号化部 (E3)
313
復号部 (D4)
314
復号部 (D1)
315
暗号化部 (E2)
316
装置ID 格納部
317
装置固有鍵 生成部
318
ソフトID 取得部
319
署名検証部 (VRF)
320
ソフトウエア 格納部
暗号化 ソフトウエア
321
制御部
322
表示部
323
入力部
324
ソフトウェア実行部
325
復号部 (D2)
326
乱数 格納部
メモリーカード
200c
耐タンパモジュール部
210
211
認証部
212
復号部 (D3)
213
暗号化部 (E4)
214
判定部
215
216
暗号化部 (E5)
217
キー情報 記憶部
キー情報
復号部 (D5)
220
221
暗号化 ソフトウエア
第1記憶領域
情報記憶部
231c
暗号化 ソフトウエア 管理情報 テーブル
第2記憶領域
222

【図１４】


300d
情報処理装置
200d
210
耐タンパモジュール部
211
認証部
212
復号部
(D3)
213
暗号化部
(E4)
214
判定部
218
情報
記憶部
220
221
暗号化
ソフトウエア
第1記憶領域
情報記憶部
222
231
ソフトウエア
管理情報
テーブル
第2記憶領域
メモリーカード

【図１５】


部分ソフトウェア管理テーブル
219
部分ソフトウェア管理情報
ソフトID(SID1)
前半ソフト署名データ
ソフトウェア管理情報テーブル
231
ソフトウェア管理情報
241d
ソフトID(SID1)
ソフトキー(XYZ123)
インストール回数情報(10)
後半ソフト署名データ
装置ID(＃1)
装置ID(＃1)

【書類名】　要約書

【要約】

【課題】　記録媒体上の改竄がされにくく、インストールの対象の端末装置と記録媒体との間の通信路における不当な攻撃を避けることができ、またソフトウェアとライセンス情報との対応関係を不正に更新することができない記録媒体を提供する。

【解決手段】　記録媒体は、セキュア記憶領域及び通常記憶領域を含む情報記憶部と、耐タンパモジュール部とを備えている。通常記憶領域には、ソフトウェアが、セキュア記憶領域には、前記ソフトウェアの使用許可数を示すライセンス数と、前記ソフトウェアの署名データとが対応付けて記録されている。耐タンパモジュール部は、端末装置との間で相互に機器認証を行い、セキュア記憶領域のライセンス数が所定数以内であれば、ソフトウェアと署名データとを端末装置へ出力する。

【選択図】　図３

特願２００３－０４５１０７

出願人履歴情報

識別番号　[０００００５８２１]

１．変更年月日　１９９０年　８月２８日
[変更理由]　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社